User's Guide

Avaya P130

Workgroup Switch

Software Version 2.9

July 2002

AVAYA

Contents

List of Figures

List of Tables

Overview

P130 Family Features

The P130 family is a line of easy-to-use, cost-effective workgroup 10/100M switches which allow you to build smart network edge/small workgroup solutions.

The P130 line includes the following fixed-configuration Layer-2/Multilayer Policy workgroup switches:

- P133T – twenty-four 10/100BaseTX ports.
- P133F2 – twenty-four, 10/100BaseTX and two 100BaseFX ports.
- P133G2 – twenty-four, 10/100BaseTX and two GBIC SFP (Small Form Pluggable) ports.
- P134G2 – fourty-eight, 10/100BaseTX and two GBIC SFP ports.
- P133GT2 – twenty-four, 10/100BaseTX and two 100/1000BaseT ports.

The P130 switches have the following features:

— Auto-Negotiation
— Link Aggregation Groups (LAG)
— 802.1Q VLAN
— QoS and Priority Support
— LAG and Link (Port) Redundancy
— Spanning Tree
— Congestion Control
— IP Multicast Filtering (IGMP Snooping)
— Port Mirroring
— Switch Configuration File
— Software Download
— Three options for Network Management

- The P130 uses Multilayer Policy technology to provide advanced policy-based networking (with the purchase of an Multilayer Policy License). The policies are used to enforce the Quality of Service (QoS) of IP packets, which are sent by locally attached stations.
- You can cascade up to four P133G2 and P134G2 modules using the Avaya X130CK kit which includes low- cost integrated SFP transceivers and a 2 m cascading cable. The X130CK provides up to 2 Gbps traffic throughput between the modules.

Avaya P130 Management includes:

- CLI (same CLI as the other Cajun Campus products).
  - — Connection via RS-232, Telnet, Modem and PPP.
  - — Telnet Passwords and Embedded Radius Client.
- P130 Web-based Management
- MultiService Network Manager supports the P130 management.
- Upload/Download
  - — Configuration file (in CLI format)
  - — Software Image file (single Bank) – download only
  - — Embedded Web file (download only)
  - — Log file (upload only).

P130 Features

The standard P130 features of the switch are described below.

Auto-Negotiation

Every 10/100 port on the P130 supports Auto-Negotiation which automatically detects and supports the duplex mode and speed of a connected device. Auto-negotiation is also supported on the Gigabit Ethernet ports for flow control mode only.

This means that you can simply connect the P130 to Ethernet or Fast Ethernet equipment at full or half duplex without configuration.

Link Aggregation Group (LAG)

LAG provides increased bandwidth and redundancy for critical high-bandwidth applications such as inter-switch links and connections to servers. You can aggregate the bandwidth of up to eight 10/100Base-Tx or two 1000Base-X ports.

Load sharing ensures that if one of the port connections fails, the other connections will assume the load seamlessly. Load balancing guarantees that the traffic load at any level will be divided among all the LAG links (see also the LAG documentation module).

LAGs can be created in the switch in order to increase bandwidth and resiliency in switch-to-switch and server-to-switch connections. P133T supports up to 3 LAGs, P133G2, P133GT2 and P133F2 support up to 4 LAGs, P134G2 supports up to 6 LAGs.

Each LAG is considered a single switch interface. Packets are not forwarded between its ports, and non-unicast packets are transmitted only through one port - the "Flood"(or "Base") port. In addition, packet order is maintained within each session.

The packets are distributed between ports in a LAG according to Source-MAC & Destination-MAC addresses. Three Least Significant Bits (LSB) of MAC source address are logically XOR-ed with 3 LSBs of MAC Destination Address. This scheme ensures enhanced load balancing of the traffic, sent out through the LAG ports.

You can manually configure a LAG using the CLI or a Management application. When initially created, the LAG will inherit all parameters from the Base (the 1st configured) port. These include Admin State (enable/disable), VLAN ID, Tagging Mode, Priority Level, STA Enable/Disable, Auto-Neg, Flow Control, Duplex and Speed. Each parameter change of the LAG interface will change this parameter in all ports in the LAG.

If a link has failed, traffic distribution continues on other ports in the LAG. The port is still configured as a member in the LAG and resumes operation in case of link up.

If you manually remove the port from the LAG, the port will automatically become disabled. You can then change any of the port's configuration parameters.

To set up a LAG or show an existing LAG configuration see the `set/show channel` commands in the CLI Chapter.

VLANs

The P130 suports 62 VLANs out of 4K tagged /untagged VLANs [1…4079]. All VLANs are fully IEEE 802.1Q compliant (VLANs [4080…4095] reserved for internal use).

The P130 has Standard VLAN MIB support.

Multiple VLANs per Port

The P130 provides the ability to set multiple VLANs per port. The two available Port Multi-VLAN binding modes are:

- **Bound to Configured** - the port supports all the VLANs configured in the switch/stack. These may be either Port VLAN IDs (PVID) or VLANs that were manually added to the switch.
- **Statically Bound** - the port supports VLANs manually configured on it.

QoS and Priority Support

The P130 supports end-to-end QoS and provides the following tools:

- **Queuing** - Four egress queues per port
- **Port Priority** - Transparent IEEE 802.1p and per port basis
- **Scheduling** - Weighted Round Robin

LAG and Link (Port) Redundancy

Redundancy can be implemented between any two ports in a switch. You can also assign redundancy between any two LAGs in the switch or between a LAG and a port.

Spanning Tree

The P130 implements the IEEE 802.1D Spanning Tree (STP) algorithm in order to allow backup paths and prevent loops throughout the Physical LAN. Spanning Tree is not available when redundant links are defined.

The P130 supports Spanning Tree per port as well as Spanning Tree per module, as may be required on the network.

Note: You cannot configure both Port Redundancy and Spanning Tree on an individual P130 switch.

Congestion Control

Congestion control is a key element of maintaining network efficiency as it prevents resource overload.

The P130 supports congestion control on all Ethernet ports, using the following:

- Head Of Line (HOL) Blocking Prevention
- IEEE 802.3x Flow Control in full duplex mode.

Advanced Congestion Control (Broadcast storm control)

Limits broadcast, multicast, and unknown packet traffic that traverses the switch.

IP Multicast Filtering (IGMP Snooping)

The IP Multicast Filtering uses the IGMP Snooping protocol to send a single copy of an IP packet to multiple destinations, and can be used for various applications including video streaming and video conferencing. This protocol reduces network congestion and allows more efficient switching of IP multicast traffic (see also the IP Multicast documentation module).

On Local Area Networks (LANs), IP Multicast packets are transmitted in MAC Multicast frames. Traditional LAN switches flood these Multicast packets to all stations in the VLAN. Multicast filtering functions may be added to the Layer 2 switches to avoid sending Multicast packets where they are not required. Layer 2 switches capable of Multicast filtering send the Multicast packets only to ports that connect members of that Multicast group. This is typically based on IGMP.

Port Mirroring

The P130 has a built-in ”mirroring” capability, that allows forwarding of all the traffic to/from specific ”copy source” to a ”copy destination” (also called a probe-port or sniffer-port), excluding errors and frames with errors.

When you require detailed information about the traffic at a particular port, rather than attaching an expensive analyzer to each port (or moving such a probe from port to port), the network administrator may attach an external probe to any P130 port defined as a destination port and analyze any switched port by mirroring its Rx/Tx or Tx only traffic to that destination port.

Note: Port Mirroring must be configured individually for each P130 switch.

Switch Configuration File

The Configuration File feature allows the user to read the P130 configuration parameters and save them to a file on the station. The switch configuration commands in the file are in CLI format. The user can edit the file (if required) and re-configure the P130 by downloading the configuration file. Although the file can be edited, it is recommended to keep changes to the file to a minimum.
TVisability™ MultiService Network Manager Software Update Manager
(CajunView™ UpdateMaster)
and/or the CLI.

Software Download

Safe S/W download procedure – backup code always present.

P130 Network Management

Comprehensive network management as a key component of today’s networks. Therefore we have provided multiple ways of managing the P130 to suit your needs.

P130 Device Manager (Embedded Web)

The built-in P130 Device Manager (Embedded Web Manager) allows you to manage a P130 switch using a Web browser without purchasing additional software. This application works with the Microsoft® Internet Explorer and Netscape® Navigator web browsers and Sun Microsystems Java™ Plug-in.

P130 Command Line Interface (CLI)

The P130 CLI provides a terminal type configuration tool for local or remote configuration of P130 features and functions.

MultiService Network Manager™

When you need extra control and monitoring or wish to manage other Cajun Campus equipment, then the Visability™ MultiService Network Manager suite is the answer. This suite provides the ease-of-use and features necessary for optimal network utilization.

- Visability™ MultiService Network Manager Software operates under HP OpenView, for Windows® 2000/NT® or Solaris.
- Visability™ MultiService Network Manager Software operates in standalone mode for Windows® 2000/NT®.

Avaya P130 Network Monitoring

RMON MIBs - RFC 1757

- RMON support for groups 1,2,3 and 9:
  - Statistics
  - History
  - Alarms
  - Events

SMON MIBs - RFC 2613

- SMON support for groups:
  - Data Source Capabilities
  - Port Copy
  - VLAN and Priority Statistics

Port Mirroring

The Avaya P130 provides port mirroring for additional network monitoring functionality. You can filter the traffic and mirror either outgoing traffic from the source port or both incoming and outgoing traffic. This allows you to monitor the network traffic you need.

SMON

The P130 supports Avaya's ground-breaking SMON Switched Network Monitoring, which the IETF has now adopted as a standard (RFC2613). SMON provides an unprecedented top-down monitoring of switched network traffic at the following levels:

- Enterprise Monitoring
- Switch Monitoring
- VLAN Monitoring
- Port-level Monitoring

This top-down approach gives you rapid troubleshooting and performance trending to keep the network running optimally.

Note: Visability™ MultiService Network Manager Software is required to run SMON monitoring.

Note: You need to purchase one SMON License per Avaya P130 stack.

Avaya P130 Standards Supported

The P130 complies with:

IEEE

- 802.3x Flow Control on all ports
- 802.1Q VLAN and Priority Tagging
- 802.1D Bridges and STA
- 802.3 Ethernet ports
- 802.3u Fast Ethernet ports
- 802.3z Gigabit Ethernet ports
- 802.3ab Gigabit over Copper (1000 BaseT)

IETF

- MIB-II - RFC 1213
- Bridge MIB for Spanning Tree - RFC 1493
- Time Protocol - RFC 0868
- SNMPv1 - RFC 1157
- PPP Internet Protocol Control Protocol (IPCP) - RFC 1332
- PPP Authentication Protocols (PAP & CHAP) - RFC 1334
- PPP - RFC 1661
- RMON support for groups 1,2 3, and 9 - RFC 1757
- SNTP - RFC-1769
- SMON - RFC 2613
- VLAN extension to Bridge MIB, Relevant MIB objects: dot1q (dot1qBase, dot1qVlanCurrent).

P130 Front and Back Panels

Front Panel LEDs

The front panel LEDs consist of Port LEDs and Function LEDs. The Port LEDs display information for each port according to the illuminated function LED. The function is selected by pressing the left or right button until the desired parameter LED is illuminated.

For example, if the COL LED is illuminated, then all Port LEDs show the collision status of their respective port. If you wish to select Rx then press the left button several times until the Rx function LED lights.

Figure 2.1 shows the P133T front panel and Figure 2.2 shows the P133F2/G2 front panel with a detailed view of the LEDs (described in Table 2.1) and pushbuttons. The RJ-45 console connector is at the bottom right.

Figure 2.1 P133T Front Panel LEDs and Switches

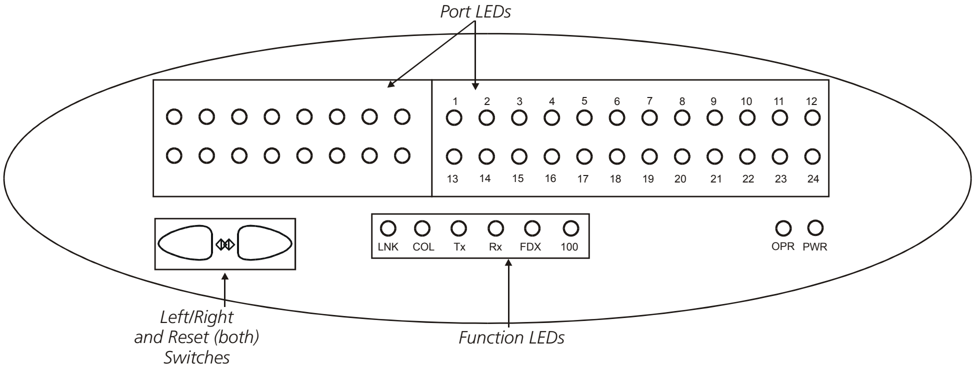


Figure 2.2 P133F2/G2/GT2 Front Panel LEDs and Switches

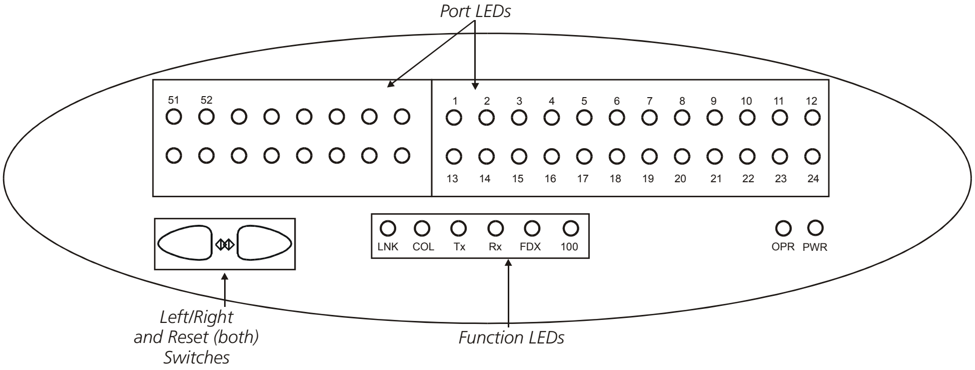
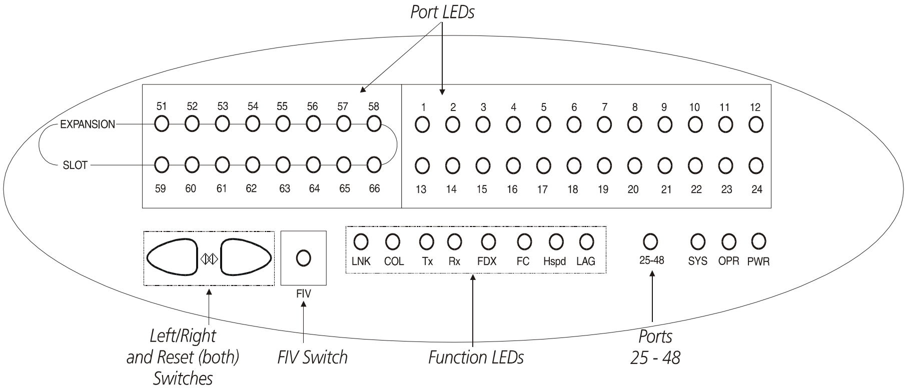


Figure 2.3 P134 Front Panel LEDs and Switches



Front Panel LEDs

Following is a Table describing P130 front panel LEDS, and the meaning of the ON, OFF and Blink (where applicable) LED status:

Table 2.1 LED Indications

LED	Function	State	Meaning
Module/Function-level			
PWR	Power Status	On	Power is up.
		Off	Power is down.
		Blink	BUPS is activated and main power is down
OPR	CPU Operational Status	On	CPU Boot and BIT operations completed
		Off	CPU is in Boot or BIT operation
LNK	Link Status	On	Link OK
		Off	No Link
COL	Collision	On	Collision occurred on line
		Off	There is no collision
25-48(*)	Port Display Mode	Off	Ports 1-24 are displayed in the Port LEDs, if selected
		On	Ports 25-48 are displayed in the Port LEDs, if selected
Tx (**)	Tx traffic	On	Packets transmission on this port
		Off	No activity on port

Table 2.1 LED Indications

Rx (**)	Rx traffic	On	Packets received on this port
		Off	No activity on port
FDX	Full Duplex Mode	On	Port in Full Duplex mode
		Off	Port in Half Duplex mode
100M	100M Speed	On	Port is working in 100M
		Off	Port is working in 10M or 1000M (Gig port)
Port-level			
1...24 ,51,52	LED per port	On	According to the function that was selected from the function-level LEDs described above
		Off	

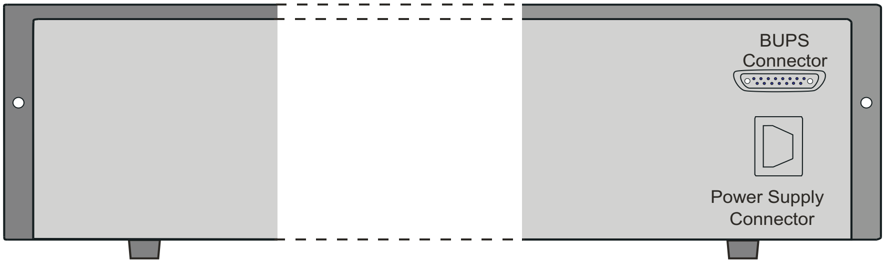
(*) This LED exists only in the P134G2

(**) Not activated for SFP Giga ports.

Avaya P130 Back Panel

The Avaya P133G2 and P134G2 back panels have Power Supply and BUPS connectors. Figure 2.4 shows the back panel of these switches.

Figure 2.4 P133G2/P134G2 AC Back Panels



BUPS Input Connector

The BUPS input connector (see Figure 2.4) is a 5 V DC connector for use with the P130 BUPS unit only.

BUPS Input

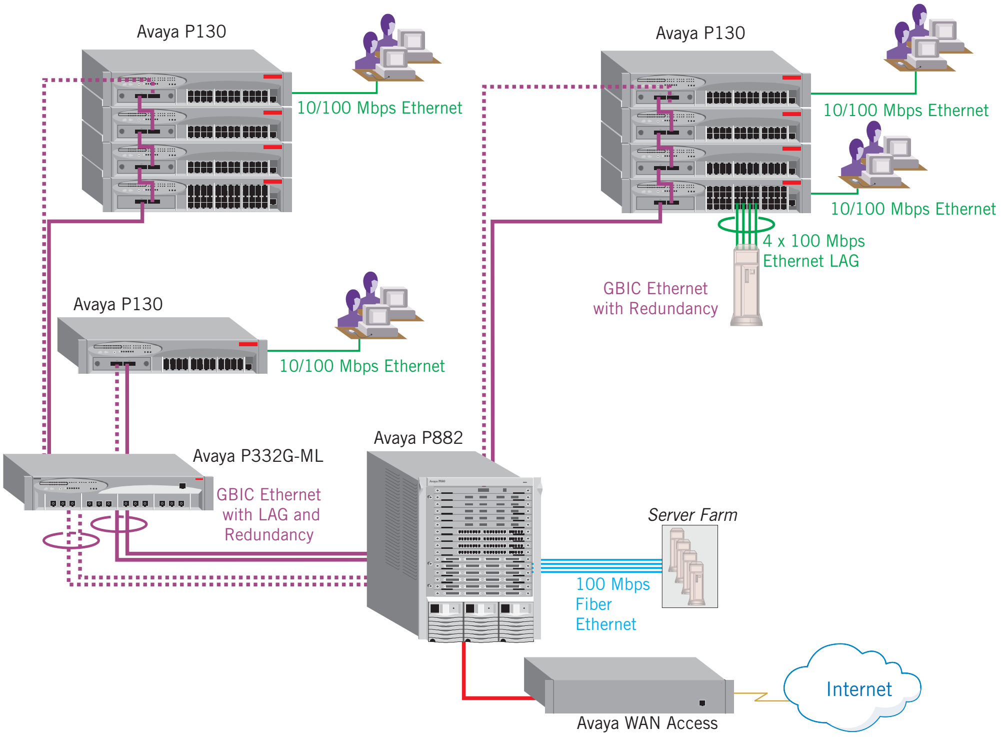
Applications

Typical Applications

The Avaya P130 is a low cost workgroup switch that is connected at the edge of the LAN. It connects end-users and servers and forwards their traffic into the core of the network.

As shown in the application below, P130 can be connected at the edge of a LAN, or stacked in a group. The P130 can be connected to the backbone or to the distribution switch using a LAG or single link connections, that can support LAG or link redundancy.

Figure 3.1 The Avaya P130 in a Network



Chapter 4

Installation and Setup

The Avaya P130 is ready to work after you carry out the installation instructions given below. All the P130 ports provide complete connectivity and no configuration is required to make the system work.

Setting up the Module

The P130 front panel contains LEDs, controls, 10/100BaseTX ports and a console connector. The status LEDs and control buttons provide at-a-glance module status information.

The P130 allows you to make the following network connections from the ports on the front panel:

- The P133G2 and P134G2 modules have two SFP (3.3 V-powered) ports for plug-in 1000BASE-SX or LX SFP GBIC Transceivers. Alternatively, you can cascade up to four P130 modules via a 2-m long Avaya X130CK cable. This proprietary low-cost cable has built-in connectors which fit directly into the SFP slot. The cable provides up to 2Gbps traffic throughput between modules.
- P133F2 has two fixed 100BASE-FX SC ports.
- P133GT2 has two fixed 100/1000BASE-T RJ-45 ports.
- P133T has no uplink ports.

Figure 4.1 Avaya P133T Module

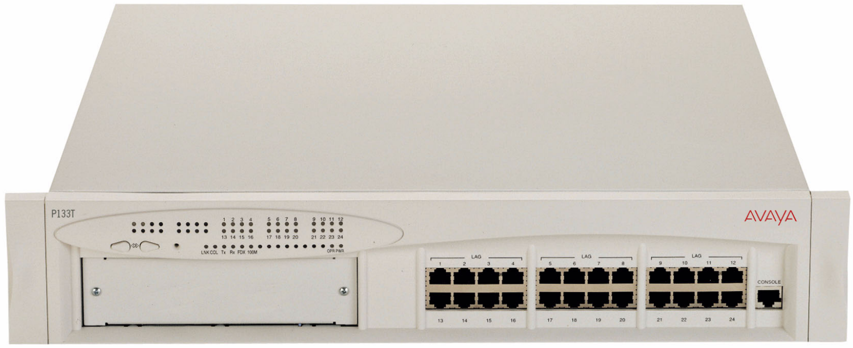


Figure 4.2 Avaya P133F2 Module

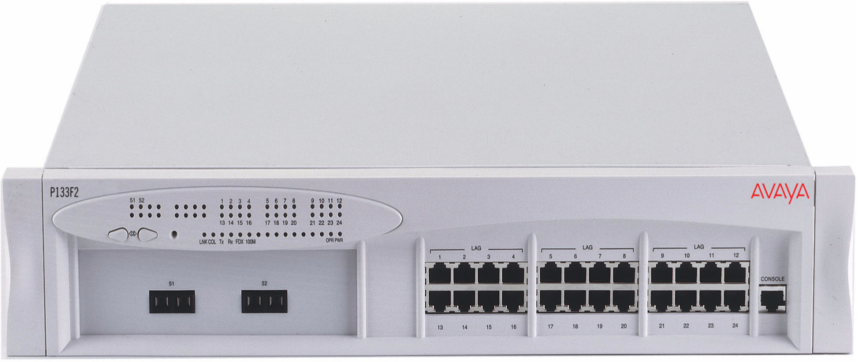


Figure 4.3 Avaya P133G2 Module

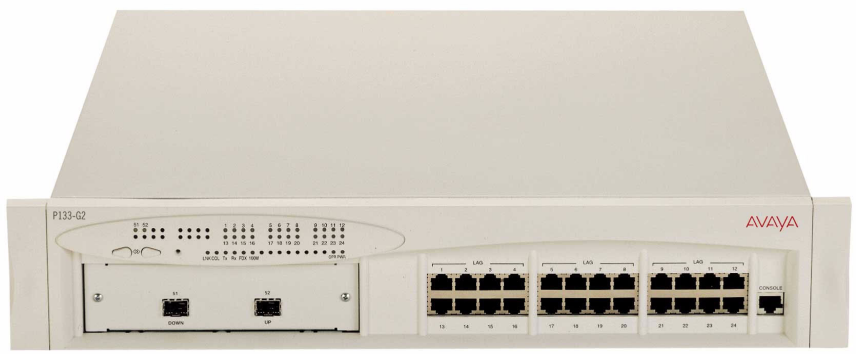


Figure 4.4 Avaya P134G2 Module

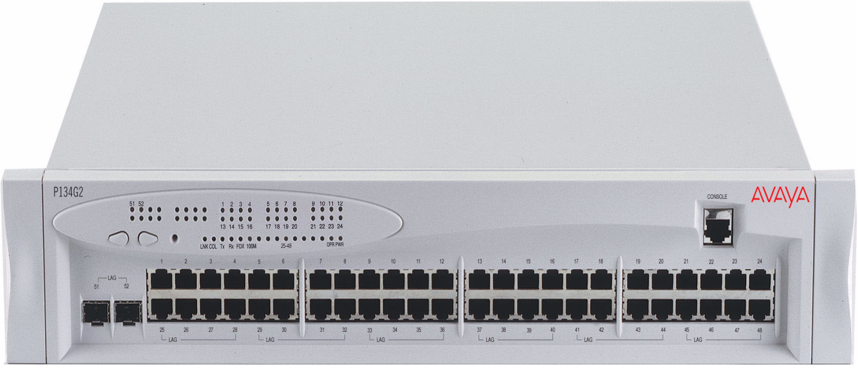
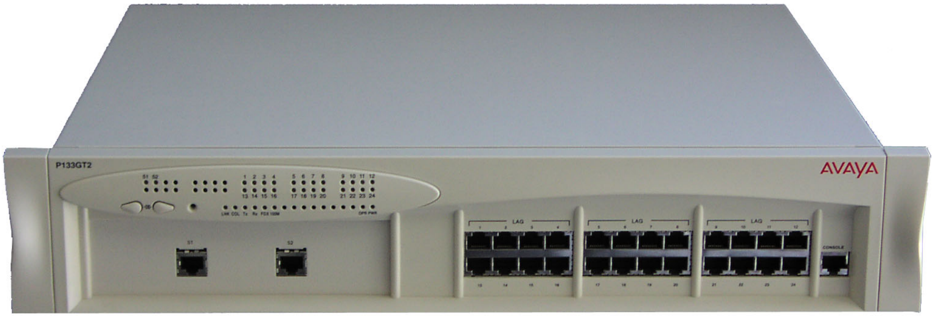


Figure 4.5 Avaya P133GT2 Module



Front-Panel Pushbuttons

Two pushbuttons, Left and Right, are used to select the function to be shown simultaneously on all Port LEDs. The current function selected is indicated by a lit Function LED.

When you press both Left and Right pushbuttons simultaneously for 1.5 seconds then the module is reset. The LEDs are described on Page 12.

Configuration Symbol

The Configuration Symbol (C/S) of the P130 module is the hardware version number and can be found either via the MultiService Network Manager application, via the CLI, or on a label on the module.

Serial Number

The P130 Serial Number is a unique number allocated to a specific P130 module. This 7-digits number is shown on a label on the module and can be found using the MIB item - genGroupSerialNumber.

Power Supply

The P130 110/220 VAC power inlet is at the back of the box.

P130/P330/P120 Back-up Power Supply (BUPS)

The P133G2 and P134G2 modules have a Back-Up Power Supply (Female D-Type connector) connector on their back panels. You can use the same BUPS unit for the P130, P330 and P120 switches.

The BUPS input is 150 W @ 5 V DC and operates in load power sharing mode with the internal P130 module power supply (See: *P133G2/P134G2 AC Back Panels* on Page 13).

Modem/RS-232

The console connector on the P130's front panel is for modem/RS-232 connections.

Whether the port functions as a Terminal or Modem port depends on the type of the connected cable, which selects either mode.

Warning: Use only the supplied configuration cable with RJ45 to D9 Serial and RJ45 to 25-pin modem adapters. For the pinouts of the connectors see: *Connector Pin Assignments* on Page 138.

Positioning

Avaya P130 can be mounted alone or you can cascade several switches in a standard 19-inch equipment rack in a wiring closet or equipment room. Up to 4 units can be cascaded in this way. When deciding where to position the unit, ensure that:

- It is accessible and cables can be connected easily and according to the configuration rule.
- Cabling is away from sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines and fluorescent lighting fixtures.
- Water or moisture cannot enter the case of the unit.
- Air-flow around the unit and through the vents in the back and sides of the case is not restricted.

Note: You must use low-cost proprietary X130CK cables to interconnect cascaded switches.

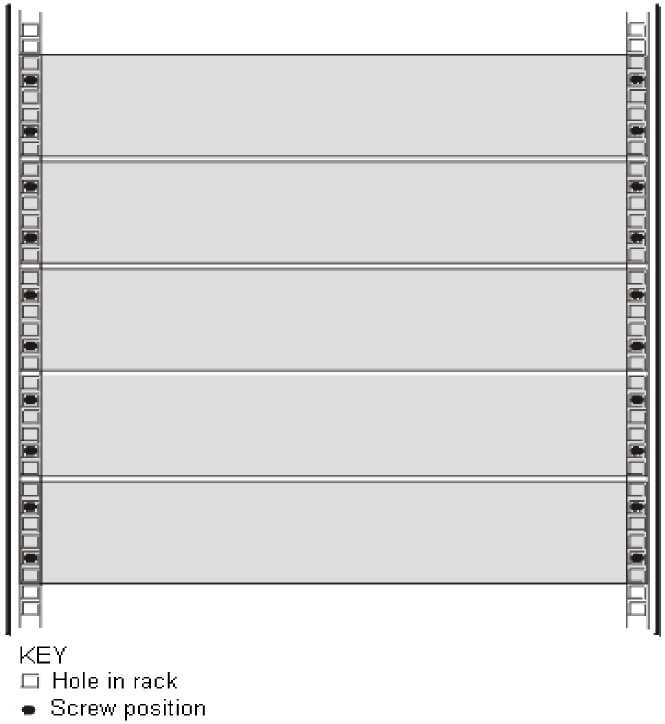
Rack Mounting

The P130 case fits in most standard 19-inch racks. P130 is 2U (88mm, 3.5”) high.

Place the P130 in the rack as follows:

1 Snap open the hinged ends of the front panel to reveal the fixing holes.
2 Insert the unit into the rack. Ensure that the four P130 screw holes are aligned with the rack hole positions as shown in Figure 4.6.

Figure 4.6 Avaya P130 Rack Mounting



3 Secure the unit in the rack using the screws. Use two screws on each side. Do not overtighten the screws.
4 Snap closed the hinged ends of the front panel.
5 Ensure that ventilation holes are not obstructed.

Connecting Cascaded Switches

Note: The information in this section only applies to the P133G2 and P134G2.

Note: The two SFP transceivers on the ends of the cable are identical. Each SFP transceiver can be connected to either an "Up" or "Down" port.

To connect cascaded switches

1 Plug one of the SFP transceivers into the port marked "52 Up" on the bottom P130 switch.

2 Plug the other SFP transceiver into the port marked "51 Down" on the P130 switch above.
The connections are illustrated in Figure 4.7.

3 Repeat Steps 1 and 2 until you reach the topmost switch.

Caution: Do not cross connect two P130 switches with two cables.

Note: You can cascade up to 4 P130 switches.

Figure 4.7 Correct Cable Connection

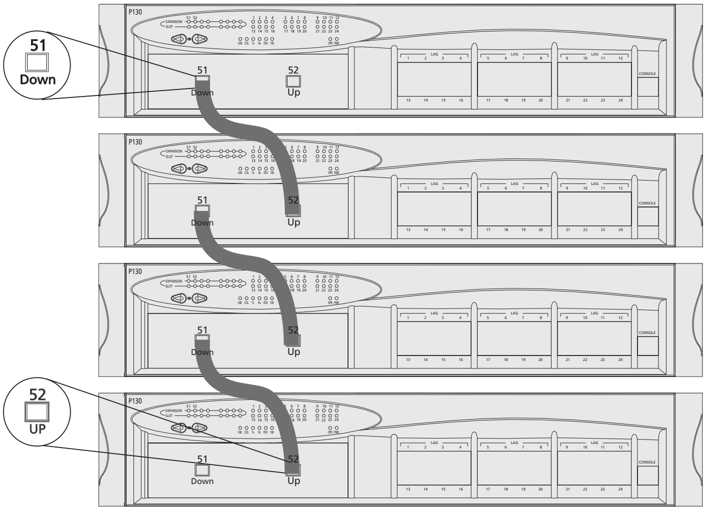
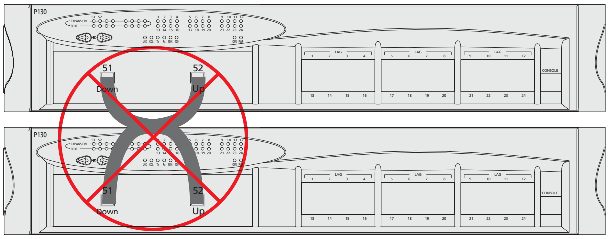


Figure 4.8 Incorrect Cable Connection



Powering On – P130 Module AC

For the AC input version of the P130, insert the power cord into the power inlet in the back of the unit. The unit powers up.

1 If you are using a BUPS, insert a power cord from the BUPS into the BUPS connector in the back of the unit. The unit powers up.

2 After power up or reset, the P130 performs a self test procedure.

Configuring the Switch

The P130 may be configured using the text-based Command Line Interface (CLI) utility, the built-in P130 Device Manager (Embedded Web) or MultiService Network Manager.

For instructions on the text-based utility, see the CLI chapter.

For instructions on installation of the graphical user interfaces, see the P130 Device Manager Appendix. For instructions on the use of the graphical user interfaces, refer to the Manager User’s Guide on the Management CD.

Avaya P130 Default Settings

The default settings for the P130 switch and its ports are determined by the P130 software. These default settings are subject to change in newer versions of the P130 software. See the Release Notes for the most up-to-date settings.

Switch Settings

Table 4.1 Default Switch Settings

Function	Default Setting
P130 IP address	149.49.32.134
Default gateway	0.0.0.0
VLANs	VLAN 1
Spanning tree	Enabled
Bridge priority for Spanning Tree	32768
NTP server IP address	0.0.0.0
Timezone offset	0 hours
Read-only SNMP community string	public
Read-write SNMP community string	public
Trap SNMP community string	public
SNMP retries number	3
SNMP timeout	2000 Seconds
SNMP authentication trap	Disabled
CLI timeout	15 Minutes

Port Settings

Table 4.2 Default Port Settings

Function	Default Port Setting		
	10/100BaseTX	**100BaseFX**	**1000BaseF**
Duplex mode	Half duplex	Full duplex	Full duplex
Speed mode	10M	100M	1000M
Flow control	Off	Off	Off
Flow control advertisement	N/A	N/A	Off
Auto-negotiation	Enabled	Not Applicable	Enabled
Administration status	Enabled	Enabled	Enabled
Port VLAN ID	1	1	1
Tagging mode	Clear	Clear	Clear
Port priority	0	0	0
Spanning Tree cost	100	20	4
Spanning Tree port priority	80 Hex	80 Hex	80 Hex

Functions operate in their default settings unless configured otherwise.

Connecting the Console Cable

The Avaya P130 has one serial port on the front panel of the switch for connecting a terminal, a terminal emulator, or a modem.

The serial port on the front panel is labelled "Console" and has a RJ-45 connector. Connect the P130 to a terminal or a terminal emulator using the supplied console cable and the RJ-45 to DB-9 adaptor. To connect a modem, use the supplied cable and an RJ-45 to DB-25 adaptor.

Note: The cable and two adaptors can be found in the accessory set, and they are clearly marked.

Configuring the Terminal Serial Port Parameters

The serial port settings for using a terminal or terminal emulator are as follows:

- Baud Rate - 9600 bps
- Data Bits - 8 bits
- Parity - None
- Stop Bit - 1
- Flow Control - None
- Terminal Emulation - VT-100

Connecting a Modem to the Console Port

A PPP connection with a modem can be established only after the Avaya P130 is configured with an IP address and net-mask, and the PPP parameters used in the Avaya P130 are compatible with the modem's PPP parameters.

1 Connect a terminal to the console port of the Avaya P130 switch as described in Connecting the Console Cable.
2 When you are prompted for a Login Name, enter the default name **`root`**.
3 When you are prompted for a password, enter the password **`root`**. You are now in Supervisor Level.
4 At the prompt, type:

```
set interface ppp <ip_addr><net-mask>
```

with an IP address and netmask to be used by the Avaya P130 to connect via its PPP interface.

Note: The PPP interface configured with the `set interface ppp` command must be on a different subnet from the stack inband interface.

5 Set the baud rate, ppp authentication, and ppp time out required to match your modem. These commands are described in the “Command Line Interface” chapter.

6 At the prompt, type:

```
set interface ppp enable
```

The CLI responds with the following:

```
Entering the Modem mode within 60 seconds...
Please check that the proprietary modem cable is plugged
into the console port
```

7 Use the DB-25 to RJ-45 connector to plug the console cable to the modem’s DB-25 connector. Plug the other end of the cable RJ-45 connector to the Avaya P130 console’s RJ-45 port.

8 The Avaya P130 enters modem mode.

9 You can now dial into the switch from a remote station, and open a Telnet session to the PPP interface IP address.

Assigning P130’s IP Stack Address

Note: All P130 switches are shipped with the same default IP address. You must change the IP address of the master P130 switch in a stack in order to guarantee that the stack has its own unique IP address in the network.

Use the CLI to assign the P130 stack/standalone switch an IP address and net mask. The network management station can establish communications with the stack/ standalone switch once this address had been assigned and the stack/standalone switch has been inserted into the network.

To assign a P130 IP stack/standalone switch address:

1 Establish a serial connection by connecting a terminal to the Master P130 switch of the stack.

2 When prompted for a Login Name, enter the default name **`root`**

3 When you are prompted for a password, enter the password **`root.`** You are now in Supervisor Level.

4 At the prompt, type:

```
set interface inband <vlan> <ip_address> <netmask>
```

Replace `<vlan>, <ip_address>` and `<netmask>` with the VLAN, IP address and net mask of the stack.

5 Press Enter to save the IP address and net mask.

6 At the prompt, type **`reset`** and press Enter to reset the stack. After the Reset, log in again as described above.

7 At the prompt, type **`set ip route`** `<dest> <gateway>` and replace `<dest>` and `<gateway>` with the destination and gateway IP addresses.

Press Enter to save the destination and gateway IP addresses.

License Key Activation

Support for Multilayer Policy, which is on top of the basic P130 Layer 2 switch features requires a license key for activation.

If no Multilayer Policy License Key was entered to the P130 switch, Policy commands will not be active. The Feature Key Certificate allows you to activate this advanced feature.

Enabling a Feature

To enable a license feature:

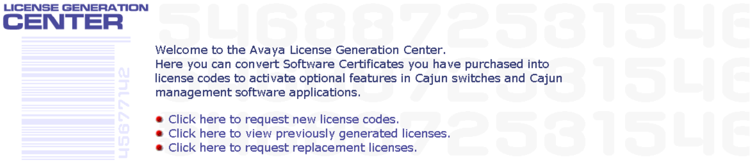
1 Purchase a Feature Key Certificate. Each Certificate is specific for:

— The Avaya switch or module.

— The required feature.

— The number of devices.

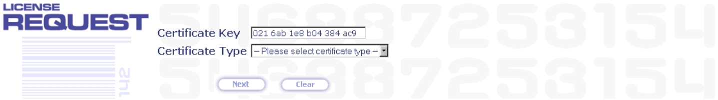
2 Go to http://license-lsg.avaya.com and click “request new license”.



Welcome to the Avaya License Generation Center.
Here you can convert Software Certificates you have purchased into license codes to activate optional features in Cajun switches and Cajun management software applications.

- Click here to request new license codes.
- Click here to view previously generated licenses.
- Click here to request replacement licenses.

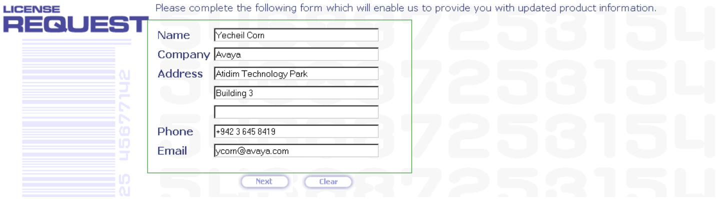
3 Enter the Certificate Key and Certificate Type.



Certificate Key: 021 6ab 1e8 b04 384 ac9
Certificate Type: – Please select certificate type –

4 Click Next.

5 Enter contact information (once per certificate)

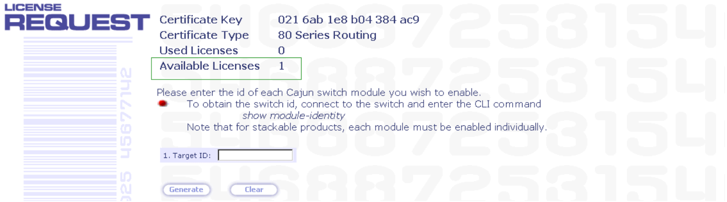


Please complete the following form which will enable us to provide you with updated product information.

Name: Yecheil Corn
Company: Avaya
Address: Atidim Technology Park
Building 3
Phone: +942 3 645 8419
Email: ycorn@avaya.com

6 Click Next.

7 View number of licenses left.

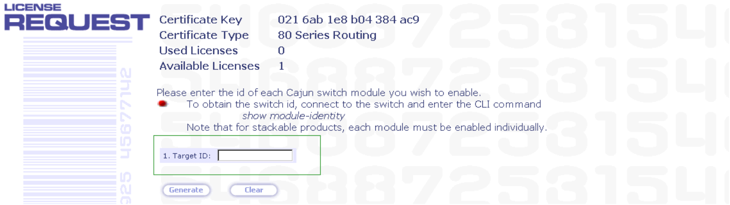


Certificate Key 021 6ab 1e8 b04 384 ac9
Certificate Type 80 Series Routing
Used Licenses 0
Available Licenses 1

Please enter the id of each Cajun switch module you wish to enable.
- To obtain the switch id, connect to the switch and enter the CLI command
  show module-identity
  Note that for stackable products, each module must be enabled individually.

1. Target ID:

8 Enter serial number of the switch(es) or module. To identify serial numbers use the CLI command: `show module-identity`.

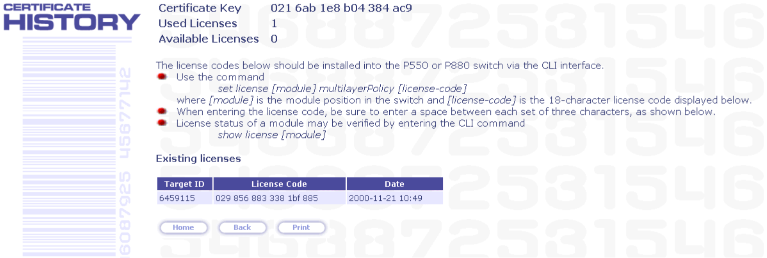


Certificate Key 021 6ab 1e8 b04 384 ac9
Certificate Type 80 Series Routing
Used Licenses 0
Available Licenses 1

Please enter the id of each Cajun switch module you wish to enable.
- To obtain the switch id, connect to the switch and enter the CLI command
  show module-identity
  Note that for stackable products, each module must be enabled individually.

1. Target ID:

9 Click Generate. The feature-enabling license code is generated



Certificate Key 021 6ab 1e8 b04 384 ac9
Used Licenses 1
Available Licenses 0

The license codes below should be installed into the P550 or P880 switch via the CLI interface.
- Use the command
  set license [module] multilayerPolicy [license-code]
  where *[module]* is the module position in the switch and *[license-code]* is the 18-character license code displayed below.
- When entering the license code, be sure to enter a space between each set of three characters, as shown below.
- License status of a module may be verified by entering the CLI command
  show license [module]

Existing licenses

Target ID	License Code	Date
6459115	029 856 883 338 1bf 885	2000-11-21 10:49

10 Enter the license code into the switch(es) or module using the `set license` CLI command.

```
set license [module] [license] [featureName]
```

where:

[module] - P130 module number

[license] - license code

[featureName] **-** smon | multilayerPolicy

and press Enter.

11 Reset the module.

12 Check that the license is activated using the CLI.
Use the `show license` CLI command.

Chapter 5

Avaya P130 CLI - Architecture, Access &Conventions

This chapter describes the Avaya P130 CLI architecture and conventions, and provides instructions for accessing the Avaya P130 for configuration purposes.

The configuration procedure involves establishing a Telnet session or a serial connection and then using the P130's internal CLI. The CLI is command-line driven and does not have any menus. To activate a configuration option, you must type the desired command at the prompt and press Enter. You can also configure your P130 using the P130 Manager with its graphical user interface. For details, see the P130 Device Manager Appendix and the MultiService Network Manager P130 Manager User Guide on the Management CD.

CLI Architecture

The P130 Switch CLI entity allows you to set and configure all Layer 2 switching and Multilayer Policy switching parameters.

Initial access to the P130 switch can be established via a serial connection of a Telnet connection to any one of the entities.

Establishing a Serial Connection

Perform the following steps to connect a terminal (physical or emulation) to the P130 Switch Console port for configuration of Stack or Router parameters:

1 Use the serial cable supplied to attach the RJ-45 console connector to any Console port of the P130 Switch. Connect the DB-9 connector to the serial (COM) port on your PC/terminal.

2 Ensure that the serial port settings on the terminal are 9600 baud, 8 bits, 1 stop bit and no parity.

3 When you see the "Welcome to Avaya P130" menu and are prompted for a Login Name, enter the default login. The default login is **`root`**.

4 When you are promoted for a password, enter the user level password **`root`**.

5 Now you can establish a connection to the switch and begin configuration of switching parameters.

Establishing a Telnet Connection

Perform the following steps to establish a Telnet connection to the Avaya P130 Switch Console port for configuration of switch parameters:

1. Connect your station to the network.
2. Verify that you can communicate with the P130 using Ping to the IP of the P130. If there is no response using Ping, check the IP address and default gateway of both the P130 and the station.
3. From the Microsoft Windows® taskbar of your PC click **Start** and then **Run** (or from the DOS prompt of your PC), then start the Telnet session by typing: **`telnet`** *`<P130_IP_address>`*
4. When you see the “Welcome to P130” menu and are prompted for a Login Name, enter the default name **`root`**
5. When you are prompted for a password, enter the User Level password **`root`** *or* **`norm`** in lower case letters (do NOT use uppercase letters). The User level prompt will appear when you have established communications with the P130.

Note: When terminating a Telnet session established from one module to another, use the **Exit** command to return to the original module.

Entering the CLI

To enter the CLI, enter your username and password. Your access level is indicated in the prompt as follows:

The User level prompt is shown below:

```
P130-N>
```

The Privileged level prompt is shown below:

```
P130-N#
```

The Supervisor level prompt is shown below:

```
P130-N(super)#
```

Conventions Used

The following conventions are used in this chapter to convey instructions and information:

- Mandatory keywords are in boldface.
- Variables that you supply are in pointed brackets <>.
- Optional keywords are in square brackets [].
- Alternative but mandatory keywords are grouped in braces {} and separated by

a vertical bar `|`.

- If you enter an alphanumeric string of two words or more, enclose the string in inverted commas.
- Information displayed on screen is displayed in `text` font.

Navigation, Cursor Movement and Shortcuts

The CLI contains a simple text editor with these functions:

Table 5.1 Navigation, Cursor Movement and Shortcuts

Keyboard	Functions
Backspace	Deletes the previous character
Up arrow/Down arrow	Scrolls back and forward through the command history buffer
Left arrow/Right arrow	Moves the cursor left or right
Tab	Completes the abbreviated command. Type the minimum number of characters unique to the command. An exception is the Reset System command which you must type in full.
Enter	Executes a single-line command
“ “	If you type a name with quotation marks, the marks are ignored.

Getting Help

On-line help may be obtained at any time by typing a question mark (**?**), or the word **`help`** on the command line or by pressing the F1 key. To obtain help for a specific command, type the command followed by a space and a question mark. Example: `P130-N(super)>` **`show?`**

Command Syntax

Commands are not case-sensitive. That is, uppercase and lowercase characters may be interchanged freely.

Command Abbreviations

All commands and parameters in the CLI can be truncated to an abbreviation of any length, as long as the abbreviation is not ambiguous. For example, `version` can be abbreviated `ver`.

For ambiguous commands, type the beginning letters on the command line and then use the Tab key to toggle through all the possible commands beginning with these letters.

Universal Commands

Universal commands are commands that can be issued anywhere in the hierarchical tree.

Top and Up commands

The `Up` command moves you up to the next highest level in the CLI command hierarchy. The `Top` command moves you to the highest level.

Retstatus command

Use the `retstatus` command to show whether the last CLI command you performed was successful. It displays the return status of the previous command.

The syntax for this command is: **`retstatus`**

Output Example:

```
P130 # set port negotiation 2/4 disable
Link negotiation protocol disabled on port 2/4.
```

Tree command

The `tree` command displays the commands that are available at your current location in the CLI hierarchy.

The syntax for this command is: **`tree`**

Chapter 6

Avaya P130 CLI

This chapter provides instructions for the configuration of your P130 using the text-based Command Line Interface (CLI or Terminal Emulation). You can also configure your P130 using the Avaya P130 Manager with its graphical user interface (see Appendix A).

The configuration procedure involves establishing a Telnet session or a serial connection and then using the P130's internal CLI. See Chapter 5 for instructions on how to establish a Telnet session or serial connection, and for a description of CLI conventions.

The CLI is command-line driven and does not have any menus. To activate a configuration option, you must type the desired command at the prompt and press Enter.

Command Groups

Following is a list of the commands groups.

General Commands

Terminal Commands

Use the `terminal width` and `terminal length` commands to set the width and length of the terminal display in characters.

The syntax for this command is:

```
terminal {width|length} [<characters>]
```

Clear screen Command

Use the `clear screen` command to clear the current terminal display.

The syntax for this command is:

```
clear screen
```

Ping Command

Use the `ping` command to send ICMP echo request packets to another node on the network.

The syntax for this command is:

```
ping [host[number]]
```

host Host IP address/Internet address of route destination. If missing then the last host IP is used.

number Number of packets to send. If missing then the last number is used

Example:

To ping the IP number 149.49.48.1 ten times:

```
P130-N> ping 149.49.48.1 10
```

```
ping 149.49.48.1 10: 56 databytes
64 bytes from 149.49.48.1: icmp_seq=0. time=8 ms
```

Tree Command

Use the `tree` command to display the commands that are available at your current location in the CLI hierarchy.

`The syntax for this command is:`

`tree`

Example:

```
P130-1#  tree
terminal width
terminal length
no hostname
no username
etc.
```

Access Level Commands

There are three security access levels – User, Privileged, and Supervisor. All access levels comply with the following restrictions:

- Read Only – only display commands are available (Show commands) to display the basic information on the device operating parameters.
- Read and Write – All of the Read Only commands and configuration commands (Set commands) used to specify and set the operation mode of the device.

User Level

The User level is a general access level used to show system parameters values. This level complies with the Read Only restrictions level.

The User level prompt indicates that the system is in User level.

Example:

```
P130-N>
```

Privileged Level

Privileged level is used by site personnel to access configuration options. This level complies with the Read and Write restrictions level.

The enable prompt indicates that the system is in Privileged level and that commands can be entered.

Example:

```
P130-1#
```

Supervisor Level

Supervisor level is used for highly secured operations such as adding a new user account, showing the PPP chap secret and also setting the device policy manager source.

The (super) prompt indicates that the system is in Supervisor level and that commands can be entered.

Example:

```
P130-N(super)#
```

Exit Command

Use the `exit` command to exit the P130 Command Line Interface (CLI).

The syntax for this command is:

```
exit
```

Tech Command

Technician level is can only be accessed from the Privileged and Supervisor levels not from the User level.

This feature is not documented and is for use by Avaya Technical Support only.

```
P130-1#
```

Account Modification Commands

Account modification commands allow you to set-up a new user account or modify an existing account of a user connected to the P130 family switch.

All account modification commands are accessed from Supervisor Level. This is the level in which you first enter the CLI.

To enter the Supervisor level, type root as the Login name and the default password `root` (in lowercase letters):

```
Welcome to P130
Login: root
Password:****
Password accepted.
P130-N(super)#
```

Username Command

Use the `username` command to add a local user account. By default there is only a single user account, named ‘root’, with password ‘root’, which access the administrator level. This basic account cannot be modified, but you can modify its basic password.

The syntax for this command is:

```
username <name> password <passwd> [access-type {read-only |
read-write | admin}]
```

`<name>`	Minimum 4 characters, maximum 12.
`<passwd>`	4 to 8 characters, for being compatible with PPP.

Example:

```
P130(super)# username john password johnny access-type read-
write
User account added.

P130(super)# username root password sodot access-type read-
write
ERROR: User account root has always an administrator access
type.

P130(super)# username root password sodot access-type admin
User account modified.
```

No Username Command

Use the `no username` command to delete a local user account. You cannot delete the supervisor level account.

The syntax for this command is:

no username <name>

Example:

```
P130(super)# no username john
User account removed.

P130(super)# no username root
ERROR: User account root cannot be removed. Command rejected.
```

Show Username Command

Use the `show username` command to display all local user accounts information.

The syntax for this command is:

show username

Example:

```
P130-N(super)# show username

User account              password          access-type
--------------            -----------------------------
john                      johnny             read-write
root                      sodot                   admin
```

License Commands

License commands allow you to show and set licenses for the P130 Switch family.

Multilayer Policy Licensing

Support for Multilayer Policy, which is on top of the basic P130 Layer 2 switch features requires a license key for activation.

If no Multilayer Policy License Key was entered to the P130 switch, the Policy CLI Commands will not be activated.

Show License Command

Use the `show license` command to display the License Key (if entered) and its supported applications (SMON, Multilayer Policy).

The syntax for this command is:

```
show license [module]
```

module	Module number

Example:

```
P130-N> show license
Mod   Application       License Key                    State      Feature Flag
---  -------------     --------------------            -------      ----------
 1    smon              0000 0000 0000 0000 0000 0000    unlicensed     0
 1  multilayerPolicy    026  1c9  e21  34f  8bb  3e8     licensed       1
```

Set License Command

Use the `set license` command to activate the Multilayer Policy or SMON capability of the P130. See Enabling a Feature on page 26 for details.

The syntax for this command is:

```
set license <module> <license> <feature name>
```

<module>	P130 module number
<license>	License number
<feature name>	The name of the feature. The default is smon.

Example:

```
P130-N> set license 1 021 1ad bad ca5 8d2 ccd multilayerPolicy
```

Time-related Commands

Show time Command

Use the `show time` command to display the current switch time.

The syntax for this command is:

```
show time
```

Example:

```
P130-N> show time
10:32:34 27 JUL 2000 GMT
```

Get time Command

Use the `get time` command to retrieve the time from the network.

The syntax for this command is:

```
get time
```

Example:

```
P130-1# get time
Time is already being acquired from network!
```

Show timezone Command

Use the `show timezone` command to display the current timezone of the switch.

The syntax for this command is:

```
show timezone
```

Example:

```
P130-N> show timezone
Timezone set to 'GMT', offset from UTC is 0 hours
```

Set timezone Command

Use the `set timezone` command to assign a timezone name and set the time difference of your P130 relative to the Coordinated Universal Time (UTC / GMT). The minutes parameter can only be set to 30.

The syntax for this command is:

```
set timezone <zone name> <hours|hours:min>
```

Example:

```
P130-1# set timezone GMT -3:30
Timezone set to 'GMT', offset from UTC is -3:30 hours
```

Clear timezone Command

Use the `clear timezone` command to return the timezone to its default, Coordinated Universal Time (UTC).

The syntax for this command is:

```
clear timezone
```

Example:

```
P130-1# clear timezone
Timezone name and offset cleared.
```

Set time protocol Command

Use the `set time protocol` command to set the protocol for use in the system as either SNTP protocol or time protocol.

The syntax for this command is:

```
set time protocol  [sntp-protocol|time-protocol]
```

Example:

```
P130-1# set time protocol sntp-protocol
The protocol has been set to SNTP protocol

P130-1#  set time protocol time-protocol
The protocol has been set to TIME protocol
```

Set time client Command

Use the `set time client` command to enable or disable the Time Client mode.

The syntax for this command is:

```
set time client [enable | disable]
```

Example:

```
P130-1(super)# set time client enable
Time client mode enable.

P130-1(super)# set time client disable
Time client mode disabled
```

Set time server Command

Use the `set time server` command to set the IP address for the time server.

The syntax for this command is:

```
set time server <IP address>
```

Example:

```
P130-1(develop)# set time server 1.2.3.4
The Server Ip has been set to 1.2.3.4
```

Show time parameters Command

Use the `show time parameters` command to display the current settings for all time related parameters.

The syntax for this command is:

```
show time parameters
```

Example:

```
P130-1(develop)# show time parameters

Client status: Enabled
Current time : 03:43:43 04 JUL 2002 UTC
Timezone set to 'UTC', offset from UTC is 0 hours
Time-Server  : 1.2.3.4
Time acquired from Time-Server: 149.49.54.192
Time protocol set to          : TIME protocol
```

System Status Commands

System status commands allow you to show and set P130 Switch system definition, image version and module/ interface information.

Show system Command

Use the `show system` command to display the uptime, system name, location, and contact person.

The syntax for this command is:

```
show system
```

Example:

```
P130-N> show system
Uptime d,h:m:s
------------------------
0,2:40:55

System Name          System Location  System Contact
-----------          ---------------  --------------
P130T_version_2.0.3  Alpha LAB        Jack
Switch MAC address
------------------
00 40 0d 8a 04 b4
```

Set system location Command

Use the `set system location` command to set the mib2 system location MIB variable. A string of 2 words or more must be type inside inverted commas - e.g. 'Operations Floor'

The syntax for this command is:

```
set system location [string]
```

string	Location string. The location is cleared if this field is blank.

Set system name Command

Use the `set system name` command to set the mib2 system name MIB variable.

The syntax for this command is:

```
set system name [string]
```

string	Name string. The name is cleared if this field is blank.

Set system contact Command

Use the `set system contact` command to set the mib2 system contact MIB variable.

The syntax for this command is:

```
set system contact [string]
```

string	System contact string. The system contact is cleared if this field is blank.

Show image version Command

Use the `show image version` command to display the software version of the image of a specified module.

The syntax for this command is:

```
show image version [mod_num]
```

[mod_num]	Module number

If a module number is not specified, the image version of all the modules will be displayed.

Example:

```
P130-N> show image version
Mod     Module-Type                                           Bank  Version
------  -----------                                           ----  -------
1       Policy capable switch, 24 10/100BaseT and 2 GBIC ports   A   1.1.5
```

Show interface Command

Use the `show interface command` to display information on the management interfaces.

The syntax for this command is:

```
show interface [{ppp | inband}]
```

```
Example:
P130-N> show interface
Interface Name  VLAN    IP address         Netmask
--------------  ----  ---------------  ---------------
inband          1     149.49.34.211    255.255.255.0
ppp             1     0.0.0.0          0.0.0.0
```

Set interface Command

Use the `set interface` command to configure the in-band interfaces on the switch.

The syntax for this command is:

```
set interface [name][vlan][ip_addr][netmask]
```

name	Interface name ("inband" used for Master agent)
vlan	The number of the VLAN to be assigned to the interface
ip_addr	IP address
netmask	Subnet mask

Show log Command

Use the `show log` command to display Log files of all modules or of a specific module.

The syntax for this command is:

```
show log [<module>[-<last module>]]
```

[<module>[-<last module>]]	One or more module numbers

Example:

To display the Log file of module number 1:

```
P130-N> show log 1
Module #1 reset events log
--------------------------
177 1 p130_sw_module.cpp 193 3849 9.9.1 1 8041dbc0 0 8003975c
eeeeeeee eeeeeeee
```

Example:

To display the Log files of modules numbered 1 and 2 in a stack:

```
P130-N> show log 1-2
```

Example:

To display the Log files of all modules:

```
P130-N> show log
```

Clear log Command

Use the `clear log` command to delete the Log file of a module.

The syntax for this command is:

`clear log` `[<module>[-<last module>]]`

[<module>[-<last module>]]	One or more module numbers

Example:

To delete the Log file of module number 1:

```
P130-N> clear log 1
Reset events log of module #1 was cleared !
```

Example:

To delete the Log files of modules numbered 1 and 2 in a stack:

```
P130-N> clear log 1-2
```

Example:

To delete the Log files of all modules:

```
P130-N> clear log
```

Show module Command

Use the `show module` command to display module status and information.

The syntax for this command is:

```
show module [module]
```

module	Module number (optional). If you do not specify a number, all modules are shown.

Example:

```
P130-N> show module
Mod Type                C/S     S/N             Statuses
--- ------------------- ------- --------------- ----------------------------
 1  P133G2              1.0     1234567         PS:ok Mode:L2
    Cascading Ports                             Conn-UP:none Conn-Down:none
    BUPS                notPresent
```

Output Fields:

Mod	Module number
`Type`	Module description/BUPS type
`C/S`	(Hardware) Configuration Symbol of the module
`S/N`	Serial number of the module
`Statuses`	Statuses of P.S., Mode, types and Connection

Show module-identity Command

Use the `show module-identity` command to see identifiers required for requesting license-keys.

The syntax for this command is:

```
show module-identity [module]
```

module	Module number

Example:

```
P130-N> show module-identity
Mod   Module Identity
---   ---------------
  1   4297236
```

Show module-config Command

Use the `show module-config` command to view the module configuration. This command applies to the Master only.

The syntax for this command is:

`show module-config`

Example:

```
P130-N> show module-config
!#
!# Upload time:              17:25:54 10 SEP 2000 GMT
!#
!# System description:       Avaya - P130 RL2 switch, SW version
1.0.0
!#
!# IP address, netmask:      149.49.34.218, 255.255.255.0
!#
!# Module #:                 1
!#
!# Module type:              P133G2
!#
!# Module-CS:                0.1
!#
!# MAC address:              00-40-0d-98-22-03
!#
!# Serial #:                 4297238
!#
!# SW version - bank A:      1.1.0
!#
!# Number of ports:          26
etc...
```

Show keep alive Command

Use the `show keep alive` command to view the keep alive interval.

The time value is in seconds.

The syntax for this command is:

```
show keep alive
```

Example:

```
P130-1# show keep alive
Keep Alive interval is: 5
```

Show timeout Command

Use the `show timeout` command to display the amount of time the CLI can remain idle before timing out in minutes. If the result is 0, there is no timeout limit.

The syntax for this command is:

```
show timeout
```

Example:

```
P130-N> show timeout
CLI timeout is 10 minutes
```

Set logout Command

Use the `set logout` command to set the number of minutes until the system automatically disconnects an idle session.

The syntax for this command is:

```
set logout <timeout>
```

<timeout>	Number of minutes (0 to 999) until the system automatically disconnects an idle session. Setting the value to 0 disables the automatic disconnection of idle sessions (default is 15 minutes).

Example:

To set the number of minutes until the system disconnects an idle session automatically:

```
P130-1# set logout 20
Sessions will be automatically logged out after 20 minutes of
idle time.
```

To disable the automatic disconnection of idle sessions:

```
P130-1# set logout 0
Sessions will not be automatically logged out.
```

Retstatus Command

Use the `retstatus` command to show whether the last CLI command you performed was successful. It displays the return status of the previous command.

The syntax for this command is:

`retstatus`

Example:

```
P130-1# set port negotiation 2/4 disable
Link negotiation protocol disabled on port 2/4.
P130-1# retstatus
Succeeded
```

Hostname Command

Use the `hostname` command to display or change the Command Line Interface (CLI) prompt. The current module number always appears at the end of the prompt.

Use the `no hostname` command to return the CLI prompt to its default.

The syntax for this command is:

`[no] hostname` `[<hostname_string>]`

<hostname_string>	**none –** displays current hostname **string –** the string to be used as the hostname (up to 20 characters).

Example:

```
P130-1# hostname
Session hostname is 'P130'
P130-1#
P130-1#  hostname ran
ran-1#
ran-1# no hostname
P130-1#
```

Show running-config Command

Use the `show running-config` command to display the currently running configuration of the module.

This command applies to Policy only.

The syntax for this command is:

```
show running-config
```

Example:

```
P130-N>  show running-config
! Avaya P130 Switch-Multilayer Policy configuration
! version 2.9.1
P130-N>
```

Show startup-config Command

Use the `show startup-config` command to display the startup configuration of the module.

This command applies to Policy only.

The syntax for this command is:

```
show startup-config
```

Example:

```
P130-N> show startup-config
! Avaya P130 Switch-Multilayer Policy configuration
! version 2.9.1
P130-N> P130-1(super)#
```

Show stack-config Command

Use the `show stack-config` command to display the stack configuration.

The syntax for this command is:

```
show stack-config
```

Example:

```
P130-N> show stack-config
!#****************************************************
!# Upload time:              11:11:33 31 JAN 2001 GMT
!# System description:       Avaya Stack of P130 workgroup switches
!# IP address, netmask:      149.49.48.109, 255.255.255.0
!# Master module #:          1
```

Download/Upload Commands

Dir Command

The `dir` command is used to show the file types that have been downloaded to the module.

The syntax for this command is:

```
dir [<mod_num>]
```

<mod_num>	Module number

Example:

```
P130-N> dir
M# file             ver num  file type     file location  file description
-- ----            --------  ----------    -------------  ----------------
1  p130             1.1.5    SW RT Image   Flash Bank A   Software Image
1  W133T            1.0.2    SW Web Image  Flash Bank A   Web Image
1  module-config    N/A      Running Conf  Nv-Ram         module configuration
```

Output Fields:

Field	Description
M#	Module number
file	There are several files loaded into modules memory: • module-config - file which contains the configuration settings made to the module. • stack-config - file which contains the configuration settings made at the stack level (e.g. IP address of the stack). • startup-config – file which contains the multilayer policy configuration settings made to this module. • running-config - file which contains the multilayer policy configuration currently in use. • p130 - file which contains the module software. • W133T – file which contains the Device Manager (Embedded Web) software. • policy-startup - For internal use only. • policy-running - For internal use only.
ver num	S/W Version number – relevant only for the Device Management S/W

file type	There are several file types: • Startup Conf - the configuration used at startup. • Running Conf – the configuration currently in use. • SW Web Image – Device Manager S/W archive file
file location	Type of internal memory into which the file is loaded
file description	Description of the file

Note: If the N/A is displayed for the EW_Archive file this means that the Device Manager S/W is not loaded correctly. Download the Device Manager S/W again.

Show tftp download/upload status Command

Use the `show tftp download status` and `show tftp upload status` commands to display the status of the current TFTP configuration file copy process into/from the device.

The syntax for this command is:

```
show tftp {download|upload} status [<mod_num>]
```

<mod_num>	Module number

Example:

```
P130-N> show tftp upload status 1
Module #1
===========
Module           : 1
Source file      : module-config
Destination file : /home/zvip/p130_module_config.txt
Host             : 149.49.39.76
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

Show tftp download software status Command

Use the `show tftp download software status` commands to display the status of the current TFTP Device Manager S/W (Embedded Web) download process into the device.

The syntax for this command is:

```
show tftp download software status [<mod_num>]
```

<mod_num>	Module number

Example:

```
P130-N> show tftp download software status
Module            : 1
Source file       : /home2/users/vkopilev/work/P130/brs_integr/
bsp_64115/vxWorks.
st_appl.bout.burn
Destination file : p130
Host              : 149.49.39.76
Running state     : Idle
Failure display   : (null)
Last warning     : No-warning
```

Copy stack-config tftp Command

Use the `copy stack-config tftp` command to upload the stack-level parameters from the current NVRAM running configuration into a file via TFTP.

The syntax for this command is:

```
copy stack-config tftp <filename> <ip>
```

<filename>	File name (full path)
<ip>	The IP address of the host

Example:

```
P130-1# copy stack-config tftp c:\conf.cfg 149.49.36.200
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show tftp upload status' command
```

Copy module-config tftp Command

Use the `copy module-config tftp` command to upload the module-level parameters from the current NVRAM running configuration into a file via TFTP.

The syntax for this command is:

```
copy module-config tftp <filename> <ip> <mod_num>
```

<filename>	File name (full path)
<ip>	The IP address of the host
<mod_num>	Module number

Example:

```
P130-1# copy module-config tftp c:\p130\switch1.cfg
192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show tftp upload status' command
```

Copy tftp stack-config Command

Use the `copy tftp stack-config` command to download the stack-level configuration from a saved file into the current NVRAM running configuration, via TFTP.

The syntax for this command is:

```
copy tftp stack-config <filename> <ip>
```

<filename>	File name (full path)
<ip>	The IP address of the host

Example:

```
P130-1# copy tftp stack-config c:\p130\switch1.cfg
192.168.49.10
```

Copy tftp module-config Command

Use the `copy tftp module-config` command to download the module-level configuration from a saved file into the current NVRAM running configuration of a module, via TFTP.

The syntax for this command is:

```
copy tftp module-config <filename> <ip> <mod_num>
```

<filename>	File name (full path)
<ip>	The IP address of the TFTP host
<mod_num>	Module number

```
Example:
P130-1# copy tftp startup-config  c:\p130\switch1.cfg
192.168.49.10 5
```

Copy tftp EW_archive Command

Use the `copy tftp EW_archive` command to download the P330 Device Manager application into the module via TFTP.

The syntax for this command is:

```
copy tftp EW_archive <filename> <ip> <mod_num>
```

<filename>	Embedded Web Manager image file name (full path)
<ip>	The IP address of the TFTP host
<mod_num>	Target module number

Example:

```
P130-1# copy tftp EW_archive c:\p130\p130web201 192.168.49.10 5
```

Copy tftp SW_image Command

Use the `copy tftp SW_image` command to update the software image and the device manager applications of a designated module.

The syntax for this command is:

```
copy tftp SW_image <image-file> EW_archive <filename><ip>
<mod_num>
```

<image-file>	Common name for the files that contain the Software Image and Embedded Web archive (full path)
<filename>	Embedded Web Manager image file name (full path)
<ip>	The IP address of the TFTP host
<mod_num>	Target module number

Example:

```
P130-1# copy tftp SW_image c:\p130\p130web101 EW_archive
c:\p130\p130web201 192.168.49.10 5
```

Copy tftp startup-config Command

Use the `copy tftp startup config` command to download a file to the P130 module startup configuration.

The syntax for this command is:

```
copy tftp startup-config <filename> <ip>
```

<filename>	File name (full path)
<ip>	The IP address of the TFTP host

Example:

```
P130-1# copy tftp startup-config  c:\p130\router1.cfg
192.168.49.10
P130-1#
```

Copy running-config tftp Command

Use the `copy running-config tftp` command to upload the RAM configuration.

The syntax for this command is:

```
copy running-config tftp<filename> <ip> <mod_num>
```

<filename>	File name (full path)
<ip>	The IP address of the host
<mod_num>	Module number

Example:

```
P130-1# copy running-config tftp c:\p333r\router1.cfg
192.168.49.10
```

Copy startup-config tftp Command

Use the `copy startup-config tftp` command to upload the NV-RAM configuration.

The syntax for this command is:

```
copy startup-config tftp<filename> <ip> <mod_num>
```

<filename>	File name (full path)
<ip>	The IP address of the host
<mod_num>	Module number

Example:

```
P130-1# copy startup-config tftp c:\p333r\router1.cfg
192.168.49.10
```

Show web aux-files-url Command

Use the `show web aux-files-url` command to display the URL/Directory from where the P130 can access the Device Management auxiliary files (for example help files).

The syntax for this command is:

```
show web aux-files-url
```

Example:

```
P130-N> show web aux-files-url
```

Set web aux-files-url Command

Use the `set web aux-files-url` command to allow the Device Manager to automatically locate the URL (the http://www address and path) of the Web server containing the Device Manager help files and Java plug-in.

Note: Ensure that the Web server is always accessible otherwise Web access to the device may take a few minutes.

The syntax for this command is:

```
set web aux-files-url <IP address/directory name>
```

Example:

```
P130-1# set web aux-files-url 149.93.47.25/emweb-aux-files
```

Copy running-config startup-config Command

Use the `copy running-config startup-config` command to copy the RAM configuration to the NV-RAM.

The syntax for this command is:

```
copy running-config startup-config
```

Example:

```
P130-1# copy running-config startup-config
Beginning copy operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show copy status' command
P130-1#
```

Erase startup-config Command

Use the `erase startup-config` command to erase the NV-RAM.

The syntax for this command is:

```
erase startup-config
```

Example:

```
P130-1# erase startup-config
```

Show erase status Command

Use the `show erase status` command to show the status of the current erase startup-config operation.

The syntax for this command is:

```
show erase status
```

Example:

```
P130-N> show erase status
Module           : 1
Source file      : startup-config
Destination file : startup-config
Host             : 0.0.0.0
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

Reset Commands

Reset Command

Use the `reset` command to restart the P130 switch. You must type the command in full.

The syntax for this command is:

```
reset {<mod_num>}
```

<mod_num>	Number of the module to be restarted

Example:

```
P130-1# reset
This command will force a switch-over to the master module and
disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
```

Nvram initialize Command

Use the `nvram initialize` command reset the P130 parameters to the factory defaults. If no options are specified for this command, only the Layer 2 parameters will be reset.

The syntax for this command is:

```
nvram initialize {switch | all}
```

switch	Resets all the switching level parameters (Layer 2 only)
all	Resets all parameters including Multilayer Policy parameters

Example:

```
P130# nvram initialize
This command will force a factory default and switch-over to
the master module and disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
host%
```

Port Commands

Show port Command

Use the `show port` command to display port status.

The syntax for this command is:

```
P130-N> show port [mod_num[/port_num]]
```

mod_num	Module number (optional). If you do not specify a number, the ports on all modules are shown.
port_num	Number of the port on the module (optional). If you do not specify a number, all the ports on the module are shown.

Example:

To display the status for port 4 on module 1:

```
P130-N> show port 1/4
Port  Name   Status   VLAN  Level  Neg    Dup.  Spd.   Type
---- -----  ------   ----- ------ -----  ----  ------ ------
1/4  NoName disabled 203   normal enable full  100M 100BaseT
```

Show Port Output Fields:

Field	Description
Port	Module and port number
Name	Name of the port
Status	Status of the port (connected, faulty, disabled)
VLAN	VLAN ID of the port
Level	Priority level of the port (normal or high)
Neg	The negotiation status of the port (enable, disable)
Duplex	Duplex setting for the port (fdx, hdx)
Speed	Speed setting for the port (10, 100, 1000)
Type	Port type, for example, 10/100BaseTX, GBIC_SX, GBIC_LX, GBIC_not present, GBIC_unknown, 1000Base-T

Show port flowcontrol Command

Use the `show port flowcontrol` command to display per-port status information related to flow control.

The syntax for this command is:

```
show port flowcontrol [mod_num/port_num]
```

mod_num	Module number (optional).
port_num	Number of the port on the module (optional). If you do not specify a number, filters configured on all the ports on the module are shown.

Example:

To display the flow-control port status and statistics:

```
Console> show port flowcontrol
Port    Send-Flowcontrol    Receive-Flowcntl
          Admin Oper          Admin Oper
-----   ------- ------      ------- -----
1/2       off   off           off   off
1/3       on    on            off   off
etc.
```

Output Fields:

Field	Description
Port	Module and port number
Send- Flowcontrol-Admin	Send flow-control administration. Possible settings: - on indicates the local port is capable of sending a flow control advertisement to the far end; - off indicates the local port is not capable of sending a flow control advertisement to the far end
Send- Flowcontrol-Oper	Send flow-control operation mode
Receive- Flowcontrol-Admin	Receive flow-control administration. Possible settings: - on indicates the local port can request the far end to send flow control advertisement; - off indicates the local port cannot request the far end to send flow control advertisement
Receive- Flowcontrol-Oper	Receive flow-control operation mode

Show port auto-negotiation-flowcontrol-advertisement Command

Use the `show port auto-negotiation-flowcontrol-advertisement` command to display the flow control advertisement for a Gigabit port used to perform auto-negotiation.

The syntax for this command is:

```
show port auto-negotiation-flowcontrol-advertisement
[<mod_num>[/<port_num>]]
```

mod_num	Module number
port_num	Number of the port on the module

Example:

```
P130-N> show port auto-negotiation-flowcontrol-advertisement
1/2
Port 1/2 advertises asym-tx-only flow control capabilities.

P130-N> show port auto-negotiation-flowcontrol-advertisement
Port 1/1  does not support this feature.
Port 1/2  does not support this feature.
Port 1/3 advertises no flow control capabilities.
etc.
```

Show port trap Command

Use the `show port trap` command to display information on SNMP generic link up/down traps sent for a specific port.

The syntax for this command is:

```
show port trap [<mod_num>[/<port_num>]]
```

mod_num	Module number
port_num	Number of the port on the module

Example:

```
P130-N> show port trap 1/1
Port 1/1 up/down trap is disabled
```

Show port channel Command

Use the `show port channel` command to display Link Aggregation Group (LAG) information for a specific module or port.

The syntax for this command is:

`show port channel` `[module[/port]][info]`

module/port	Module/port number
info	Display port information

Example:

To display all LAGs in a stack (without information data):

```
P130-N> show port channel
Port   Channel Status  Channel Name
------ --------------- --------------------------------
 1/1        off
 1/2        off
 1/3        off
 1/4        off
 1/5        off
 1/6        off
 1/7        off
 1/8        off
 1/9        off
 1/10       on          lag1
 1/11       on          lag1
 1/12       off
 1/13       off
etc...
```

`Example:`

To display all members of a LAG of which port 10 is a member:

```
P130-N> show port channel 1/10
Port   Channel Status  Channel Name
------ --------------- --------------------------------
 1/10       on          lag1
 1/11       on          lag1
```

Example:

To display LAG information data for port 10 on module 1:

```
P130-N> show port channel 1/10 info
Port   Speed  Duplex  Vlan  Port      Trunk    Vlan
                            Priority  status   Binding
------ ------ ------- ----- --------- -------- --------
 1/10  10     half    1     0         off      all
 1/11  10     half    1     0         off      all
```

Show port mirror Command

Use the `show port mirror` command to display mirroring information for the switch.

The syntax for this command is:

```
show port mirror [<mod_num>[/<port_num>]]
```

mod_num	Module number
port_num	Number of the port on the module

Example:

```
P130-N> show port mirror
port mirroring
Mirroring both Rx and Tx packets from port 1/2 to port 1/4 is
enabled
```

Set port level Command

Use the `set port level` command to set the priority level of a port or range of ports on the switching bus. Packets traveling through a port set at normal priority should be served only *after* packets traveling through a port set at high priority are served. Packets traveling with a 802.1p priority header are not affected by this command.

The syntax for this command is:

```
set port level <mod_num>/<port_num> {[0-7]}
```

mod_num	Module number
port_num	Number of the port on the module

0-7	Priority level

Example:

To set the priority level for port 2 on module 1 to 7:

```
P130-1# set port level 1/2 7
Port 1/2 port level set to 7.
```

Set port negotiation Command

Use the `set port negotiation` command to enable or disable the link negotiation protocol on the specified port. This command applies to Fast Ethernet or Gigabit Ethernet ports. When negotiation is enabled, the speed and duplex of the Fast Ethernet ports are determined by auto-negotiation. If autonegotiation is disabled, you can set these port parameters using the relevant CLI commands (if autonegotiation is enabled, these commands have no effect).

The syntax for this command is:

```
set port negotiation <mod_num/port_num> {enable | disable}
```

mod_num	Module number
port_num	Number of the port on the module
enable	Enable the link negotiation protocol
disable	Disable the link negotiation protocol

Example:

To disable link negotiation protocol on port 4, module 1:

```
P130-1# set port negotiation 1/4 disable
Link negotiation protocol disabled on port 1/4.
```

Set port enable Command

Use the `set port enable` command to enable a port or a range of ports.

The syntax for this command is:

```
set port enable <mod_num/port_num>
```

mod_num	Module number
port_num	Number of the port on the module

Example:

To enable port 3:

```
P130-1# set port enable 1/3
Port 1/3 enabled.
```

Set port disable Command

Use the `set port disable` command to disable a port or a range of ports.

Note: If you have disabled a particular port but the link is still connected, the LED for that port will remain ON.

The syntax for this command is:

```
set port disable <mod_num/port_num>
```

mod_num	Module number
port_num	Number of the port on the module

Example:

```
P130-1# set port disable 1/10
Port 1/10 disabled.
```

Set port speed Command

Use the `set port speed` command to configure the speed of a port or range of ports.

In autonegotiation mode, the port's speed is determined by autonegotiation. You cannot set the speed type to 10 or 100 when autonegotiation is enabled.

The syntax for this command is:

```
set port speed <mod_num/port_num><speed>
```

mod_num	Module number
port_num	Number of the port on the module
<speed>	Set port speed to 10, or 100 Mbps

Example:

To configure port 2 on module 1 port speed to 10 Mbps:

```
P130-1# set port speed 1/2 10MB
Port 1/2 speed set to 10 Mbps.
```

Set port duplex Command

Use the `set port duplex` command to configure the duplex type of an Ethernet or Fast Ethernet port or range of ports.

You can configure Ethernet and Fast Ethernet interfaces to either full duplex or half duplex. The duplex status of a port in autonegotiation mode is determined by autonegotiation. An error message is generated if you attempt to set the transmission type of autonegotiation Fast Ethernet ports to half- or full-duplex mode.

The syntax for this command is:

```
set port duplex <mod_num/port_num> {full | half}
```

mod_num	Module number
port_num	Number of the port on the module
full	Keyword to specify full-duplex transmission
half	Keyword to specify half-duplex transmission

Example:

To set port 2 on module 1 to full duplex:

```
P130-1# set port duplex 1/2 full
Port 1/2 set to full-duplex.
P130-1#
```

Set port flowcontrol Command

Use the `set port flowcontrol` command to set the send/receive flow-control frames (whether proprietary or IEEE 802.3x) for a full duplex module port. Each direction can be configured separately.

This command is supported on Fast and Gigabit Ethernet switching ports.

The syntax for this command is:

```
set port flowcontrol {receive | send | all}<mod_num/
port_num>{off | on | prop}
```

receive	Indicates whether the port can receive administrative status from a remote device. Available only for Gigabit Ethernet modules with negotiation set to off.
send	Indicate whether the local port can send administrative status to a remote device. Available only for Gigabit Ethernet modules with negotiation set to off.
all	Send and receive (symmetric flow control).
mod_num	Module number
port_num	Number of the port on the module
off	Used with receive to turn off an attached device's ability to send flow-control packets to a local port. Used with send to turn off the local port's ability to send administrative status to a remote device.
on	Used with receive to require that a local port receive administrative status from a remote device. Used with send, the local port sends administrative status to a remote device.
prop	Proprietary flow control.

Example:

These examples show how to use the set port flowcontrol command set:

```
P130-1# set flowcontrol receive 5/1 on
Port 5/1 flow control receive administration status set to on
(port will require far end to send flowcontrol)
P130-1#

P130-1# set flowcontrol send 5/1 off
Port 5/1 flow control send administration status set to off
(port will send flowcontrol to far end)
P130-1#
```

Set port auto-negotiation-flowcontrol-advertisement Command

Use the `set auto-negotiation-flowcontrol-advertisement` command to set the flowcontrol advertisement for a Gigabit port when performing autonegotiation.

The syntax for this command is:

```
set port auto-negotiation-flowcontrol-advertisement
<mod_num>/<port_num> {no-flowcontrol | asym-tx-only | sym-only
| sym-and-asym-rx}
```

mod_num	Module number
port_num	Number of the port on the module
no-flowcontrol	The port will advertise no pause capabilities
asym-tx-only	The port will advertise asymmetric Tx pause capabilities only
sym-only	The port will advertise symmetric pause capabilities only
sym-and-asym-rx	The port will advertise both symmetric and asymmetric Rx pause capabilities.

Example:

```
P130-1# set port auto-negotiation-flowcontrol-advertisement
1/51 asym-tx-only
Port 1/51 pause capabilities was set
```

Set port name Command

Use the `set port name` command to configure a name for a port. If you do not specify a name, the port name remains empty.

The syntax for this command is:

```
set port name <mod_num>/<port_num> [<name>]
```

mod_num	Module number
port_num	Number of the port on the module
<name>	Name assigned to the port.

Example:

```
P130-1# set port name 1/21 arthur
Port 1/21 name set.
```

Set port trap Command

Use the `set port trap` command to enable/disable generic SNMP uplink / downlink traps from a port.

The syntax for this command is:

```
set port trap <mod_num>/<port_num> {enable | disable}
```

mod_num	Module number
port_num	Number of the port on the module
enable	Enables generic SNMP uplink/downlink traps from a port
disable	Disables generic SNMP uplink/downlink traps from a port

Example:

```
P130# set port trap 1/21 enable
Port 1/21 up/down trap enabled.
```

Set port channel Command

Use the `set port channel` command to enable or disable a Link Aggregation Group (LAG) interface on the module. You can also add or remove a port from an existing LAG. All ports in the LAG are configured with the base ports' parameters such as port speed, duplex mode, VLAN ID, tagging mode, priority level. When adding a port to an existing LAG, type the same LAG-name (or no LAG-name), otherwise you will get an error message. The added port must belong to the same connector group - refer to the "LAG" indication on device's front panel. When a port is removed from a LAG, it becomes disabled.

The syntax for this command is:

```
set port channel <mod_num>/<port_list> {on | off} <LAG-name>
```

<mod-num>	Module number
<port_list>	A list of ports to be aggregated, separated by commas.
<LAG_name>	Name for the LAG interface.

Example:

```
P130-1# set port channel 1/6,18 on server2
Port 1/6 channel mode set to on
Port 1/18 was added to channel
```

Set port redundancy enable/disable Command

Use the `set port redundancy` command to enable or disable the defined redundancy schemes. Using this command will not delete existing redundancy entries.

Note: You must disable Spanning Tree before you can enable redundancy.

The syntax for this command is:

```
set port redundancy {enable|disable}
```

Example:

```
P130-1# set port redundancy enable
All redundancy schemes are now enabled
```

Set port redundancy Command

Use the `set port redundancy` command to define/remove redundancy schemes between a Primary and a Secondary link. The link can be any port that does not belong to a LAG, or a LAG interface. In either case, there should not be any redundancy scheme already defined on any of the links.

The syntax for this command is:

```
set port redundancy <mod_num>/<prim_port_num> <mod_num>/
<second_port_num> {on/off} [<redundancy_name>]
```

<mod_num>	Module number
<prim_port_num>	Primary link of the redundancy scheme
<second_port_num>	Secondary link of the redundancy scheme
<redundancy_name>	Name for the redundancy scheme (optional)

Example:

```
P130-1# set port redundancy 1/7 2/12 on red1
uplink: Port 2/12 is redundant to port 1/7.
Port redundancy is active - entry is effective immediately
```

Show port redundancy Command

Use the `show port redundancy` command to display information about all redundancy schemes defined in the switch.

The syntax for this command is:

```
show port redundancy
```

Example:

```
P130-N> show port redundancy
Redundancy Name  Primary Port  Secondary Port  Status
---------------  ------------  --------------  ------
fast                 1/7            2/12       enable
uplink               1/13           3/20       enable
```

Set port mirror Command

Use the `set port mirror` command to define a port mirroring source-destination pair in the switch.

The syntax for this command is:

```
set port mirror source-port <mod_num>/<port_num> mirror-port
<mod_num>/<port_num> sampling {always | disable} direction
{rx| tx | both}
```

always	Keyword to activate the port mirroring entry
disable	Keyword to change the status of the port mirroring entry to "not ready"
rx	Keyword to copy only incoming traffic
tx	Keyword to copy only outgoing traffic
both	Keyword to copy both incoming and outgoing traffic

Example:

```
P130-1# set port mirror source-port 1/9 mirror-port 1/10
sampling always direction both
Mirroring both Rx and Tx packets from port 1/9 to port 1/10 is
Enabled
```

Clear port mirror Command

Use the `clear port mirror` command to cancel port mirroring.

The syntax for this command is:

```
clear port mirror <source-module>/<source-port>/<dest-
module>/<dest-port>
```

Example:

```
P130-1# clear port mirror 1/2/1/4
this command will delete the port mirror entry
 - do you want to continue (Y/N)?  y

Mirroring packets from port 1/2 to port 1/4 is cleared
```

Set port vlan Command

See *Set port vlan Command* on page 90.

FlowControl Commands

Set internal buffering Command

Use the `set internal buffering` command to set the size (either Maximum or Minimum) of the Receive (Rx) buffer allocated to each port of the specified module. This command is meaningless when any port of the module is operating with flow control ON. You must reset the switch after setting the internal buffering parameters.

The syntax for this command is:

```
set internal buffering <mod_num> {max|min}
```

max	Sets the internal receive buffer to its maximum size.
min	Sets the internal receive buffer to its minimum size (this is the Default).

Example:

```
P130-N> set internal buffering 1 max
Done.
```

Show internal buffering Command

Use the `show internal buffering` command to show the size options (Maximum, Minimum, or Medium) of the Receive (Rx) buffer allocated to each port of the specified module.

The syntax for this command is:

```
show internal buffering [<mod_num>]
```

<mod_num>	Module number

Example:

```
P130-N> show internal buffering 1
Module  Internal Buffer
------  ---------------
  1          med
```

Set port flowcontrol Command

See Set port flowcontrol Command on page 74

Show port flowcontrol Command

See Show port flowcontrol Command on page 67.

Spanning Tree Commands

Show spantree Command

Use the `show spantree` command to display spanning-tree information.

The syntax for this command is:

```
show spantree [<mod_num>[/<port_num>]]
```

mod_num	Module number
port_num	Number of the port on the module

Example:

```
P130-N> show spantree
Spanning tree enabled

Designated Root:  00-40-0d-88-06-c8
Designated Root Priority: 32768
Designated Root Cost: 20
Designated Root Port: 1/1
Root Max Age: 20   Hello Time: 2

Bridge ID MAC ADDR: 00-40-0d-92-04-b4
Bridge ID priority: 32768

Port   State         Cost       Priority
------ ------------- ---------- ------------
1 /1   Forwarding    20         128
1 /2   not-connected 20         128
1 /3   LAG-member    20         128
1 /4   LAG-member    20         128
1 /5   not-connected 20         128
1 /6   not-connected 20         128
etc...
```

Output Fields:

Field	Description
Spanning tree	Status of whether Spanning-Tree Protocol is enabled or disabled.
Designated Root	MAC address of the designated spanning-tree root bridge
Designated Root Priority	Priority of the designated root bridge
Designated Root Cost	Total path cost to reach the root
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges).
Root Max Age	Amount of time a BPDU packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Bridge ID MAC ADDR	Bridge MAC address used in the sent BPDUs.
Bridge ID Priority	Bridge priority
Port	Port number
State	Spanning-tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Priority	Priority associated with the port.

Set spantree Commands

Use the `set spantree` command to enable/disable the spanning-tree protocol for the P130 switch.

The syntax for this command is:

```
set spantree {enable|disable}
```

Example:

```
P130-1# set spantree enable
bridge spanning tree enabled.
```

Set spantree priority Command

Use the `set spantree priority` command to set the bridge priority for STP.

The syntax for this command is:

```
set spantree priority <bridge_priority>
```

bridge_priority	Number representing the priority of the bridge. The priority level is from 0 to 65535, with 0 indicating high priority and 65535 indicating low priority.

Example:

To set the bridge priority to 45000:

```
P130-1# set spantree priority 45000
Bridge priority set to 45000.
```

Set port spantree Command

Use the `set port spantree` command to enable/disable the spanning-tree protocol for a specific port.

The syntax for this command is:

```
set port spantree {enable|disable}[module/port]
```

Example:

```
P130-1# set port spantree enable 1/2
```

Set port spantree priority Command

Use the `set port spantree priority` command to set the port priority.

The syntax for this command is:

```
set port spantree priority  [module/port] [value]
```

value	Number representing the priority of the port. The priority level is from 0 to 255, with 0 indicating high priority and 255 indicating low priority

Example:

To set the port priority to 45000:

```
P130-1# set port spantree priority 1/2 45000
```

Set port spantree cost Command

Use the set port spantree cost command to set the port cost.

The syntax for this command is:

```
set port spantree cost [module/port] [value]
```

CAM Commands

Clear cam Command

Use the `clear cam` command to delete all entries from the CAM table.

The syntax for this command is:

`clear cam`

Example:

```
P130-1# clear cam
CAM table entry cleared.
```

Show cam Commands

Use the `show cam` commands to display the CAM table entries for a specific port or MAC Address.

The syntax for this command is:

`show cam` `[<mod_num>[/<port_num>]]`

and

`show cam mac` `<mac_addr>`

<mod_num>	Module number
<port_num>	Number of the port on the module
<mac_addr>	MAC address

Example:

```
P130-N> show cam 1/1
Dest MAC/Route Dest Destination Ports
------------------- -----------------
00-40-0d-59-03-78   1/1
00-d0-79-0a-0a-da   1/1
00-40-0d-43-1e-e9   1/1
etc...
P130-N> show cam mac 00-40-0d-88-06-c8
Dest MAC/Route Dest Destination Ports
------------------- -----------------
00-40-0d-88-06-c8    1/1
Total Matching CAM Entries Displayed = 1
```

VLAN Commands

Show trunk Command

Use the `show trunk` command to display VLAN tagging information of the ports.

The syntax for this command is:

```
show trunk [<mod_num>[/<port_num>]]
```

<mod_num>	Module number
<port_num>	Number of the port on the module

Example:

```
P130-N> show trunk 1/22
show trunk 1/22
Port   Mode  Binding mode         Native vlan Vlans allowed on trunk
------ ----- -------------------- ----------- ----------------------
 1/22  off   statically bound           1          1
```

Following are the `show trunk` command output fields:

Field	Description
Port	Module and port number(s)
Mode	Tag status of the port (ON - dot1Q tagging mode, OFF - clear mode).
Native VLAN	Number of the Port VLAN ID (the VLAN to which received untagged traffic will be assigned). If the Port is in “clear mode” only frames of this VLAN will be transmitted.
VLANs allowed on trunk	Range of values allowed on the Trunk

Set trunk Command

Use the `set trunk` command to configure the tagging mode.

The syntax for this command is:

```
set trunk <mod_num>/<port_num> {off|dot1q}
```

<mod_num>	Module number
<port_num>	Number of the port on the module
off	Forces the port to become a non-tagging port. The port is in the clear (tagging) mode: it will never send frames as tagged, but it will correctly interpret received tagged frames.
dot1q	Forces the port to become a 802.1Q tagging port. The port is in the tagging mode: it will send frames as tagged and will correctly interpret received untagged frames.

Example:

```
P130-1# set trunk 1/19 dot1q
Dot1Q VLAN tagging set on port 1/19.

P130-1# set trunk 1/19 off
No VLAN tagging set on port 1/19.
```

Clear vlan Command

Use the `clear vlan` command to delete an existing VLAN and return ports from this VLAN to the default VLAN #1. When you clear a VLAN, all ports assigned to that VLAN are assigned to the default VLAN #1.

The syntax for this command is:

```
clear vlan [VLAN_num]
```

VLAN_num	Number of the VLAN (range is 1 to 4079).

Example:

This example shows how you can delete an existing VLAN (VLAN 4) from a management domain:

```
P130-1# clear vlan 4
This command will assign all ports on VLAN 4 to their default
in the entire management domain
```

```
Do you want to continue (y/n) [n]? y
VLAN 4 deletion successful
```

Set inband vlan Command

Use the `set inband vlan` command to set a value for the management vlan (from 1 to 4079).

The syntax for this command is:

```
set inband vlan <value>
```

<value>	A VLAN number between 1 and 4079.

Example:

```
P130-1# set inband vlan 1
Management VLAN number set to 1
```

Show vlan Command

Use the `show vlan` command to display information about VLANs that exist on the switch.

The syntax for this command is:

```
show vlan [<vlan-id> | name <vlan-name>]
```

<vlan_id>	Number between 1 and 4079, identifying the VLAN.
<vlan-name>	Name of VLAN

Example:

```
P130-N> show vlan
Vlan-id Vlan-name
------- ---------
1       Vlan1
```

Set vlan Command

Use the `set vlan` command to create a VLAN (ID and Name). You must create a VLAN before you can set a port to that VLAN.

The syntax for this command is:

```
set vlan <VLAN_id> [name<VLAN-name>}
```

<VLAN_id>	Number between 1 and 4079, identifying the VLAN.
<VLAN-name>	VLAN name.

Example:

```
P130-1# set vlan 2 name vlan2
Vlan-id 2, vlan-name vlan2 created.
```

Set port vlan Command

Use the `set port vlan` command to set the Port's VLAN ID (PVID). The VLAN number must be within the range 1 to 4079.

The syntax for this command is:

```
set port vlan <VLAN_num> <mod_num>/<port_num>
```

<VLAN_num>	Number between 1 and 4079, identifying the VLAN.
<mod_num>	Module number
<port_num>	Number of the port on the module

Example:

To set VLAN 850 to include ports 4 through 7 on module 1.

```
P130-1# set port vlan 850 1/4-7
VLAN 850 modified.
VLAN  Mod/Ports
---- ----------------------
850   1/4-7
```

Set port vlan-binding-mode Command

Use the `set port vlan-binding-mode` command to define the binding method used by ports.

The syntax for this command is:

```
set port vlan-binding-mode [port_list] [value]
```

port_list	module and ports to bundle (format: module/port)
value	**static** - the port supports only the egress VLAN list as configured **bind-to-configured** - the port support the whole range of VLANs on the device

Example:

```
P130-1# set port vlan-binding-mode 1/5-15 static
Set Port vlan binding method:1/5
Set Port vlan binding method:1/6
.
```

Show port vlan-binding-mode Command

Use the `show port vlan-binding-mode` command to display port vlan binding mode information.

The syntax for this command is:

```
show port vlan-binding-mode
```

Example:

```
P130-N> show port vlan-binding-mode
port 1/1 is statically bound
port 1/2 is statically bound
etc.
```

Set port static-vlan Command

Use the `set port static-vlan` command to statically assign VLANs to ports.

The syntax for this command is:

```
set port static-vlan [module/port range] [vlan num]
```

module/port range	port range
vlan num	VLAN to bind to port

Example:

```
P130-1# set port static-vlan 1/4-6 9
```

Clear port static-vlan Command

Use the `clear port static-vlan` command to unbind vlans from a port

The syntax for this command is:

```
clear port static-vlan [module/port range] [vlan num]
```

module/port range	port range
vlan num	VLAN to unbind to port

Example:

```
P130-1# clear port static-vlan 1/4-6 9
```

Congestion Control Commands

Show broadcast storm control Command

Use the `show broadcast storm control` command to display broadcast storm status and settings.

The syntax for this command is:

```
show broadcast storm control [<module_number>[-<module_number>]]
```

<module_number> [-<module_number>]	One or more module numbers

Example:

```
P130-N> show broadcast storm control
Module    Broadcast         Threshold
          Storm Control
--------  ----------------  ------------
 1         disable           500
```

Set broadcast storm control Command

Use the `set broadcast storm control` command to enable or disable broadcast storm control.

The syntax for this command is:

```
set broadcast storm control <module_number>[-<module_number>]
{enable|disable}
```

<module_number> [-<module_number>]	One or more module numbers
{enable | disable}	enable|disable broadcast storm control

Example:

```
P130-1# set broadcast storm control 1 enable
```

Set broadcast storm control threshold Command

Use the `set broadcast storm control threshold` command to set the broadcast storm control threshold.

The syntax for this command is:

```
set broadcast storm-control threshold <module_number>[-
<module_number>] <threshold-number>
```

<module_number> [-<module_number>]	One or more module numbers
<threshold-number>	Limit number of packets per second the module ports can receive

Example:

```
P130-1# set broadcast storm-control threshold 1 500
```

Multicast Commands

Show intelligent-multicast Command

Use the `show intelligent-multicast` command to display the intelligent multicast configuration.

The syntax for this command is:

show intelligent-multicast

Example:

```
P130-N> show intelligent-multicast
Intelligent-multicast configuration:
------------------------------------
intelligent-multicast state --------------------- Disabled
Intelligent-multicast client-port-pruning time --- 600[Sec]
Intelligent-multicast router-port-pruning time ---1800[Sec]
intelligent-multicast group-filtering-delay time -  10[Sec]
```

Set intelligent-multicast Command

Use the `set intelligent-multicast` command to enable or disable the IP-multicast filtering application.

The syntax for this command is:

set intelligent-multicast {enable|disable}

Example:

```
P130-1# set intelligent-multicast enable
Done!
```

Set intelligent-multicast client-port-pruning time Command

Use the `set intelligent-multicast client-port-pruning time` command to define aging time for client ports.

The syntax for this command is:

set intelligent-multicast client-port-pruning time <time>

<time>	Time in seconds

Example:

```
P130-1# set intelligent-multicast client-port-pruning-time 20
Done!
```

Set intelligent-multicast router-port-pruning time Command

Use the `set intelligent-multicast router-port-pruning time` command to define aging time for router ports.

The syntax for this command is:

`set intelligent-multicast router-port-pruning time` `<time>`

<time>	Time in seconds

Example:

```
P130-1# set intelligent-multicast router-port-pruning time 20
Done!
```

Set intelligent-multicast group-filtering-delay time Command

Use the `set intelligent-multicast group-filtering-delay time` command to define group filtering time delays.

The syntax for this command is:

`set intelligent-multicast group-filtering-delay time` `<time>`

<time>	Time in seconds

Example:

```
P130-1# set intelligent-multicast group-filtering-delay time
20
Done!
```

IP Route Configuration Commands

Show ip route Command

Use the `show ip route` command to display IP routing table entries.

The syntax for this command is:

```
show ip route
```

Example:

```
P130-N> show ip route
Destination Gateway
----------- -----------
149.49.1.1 172.20.22.201
190.20.0.0 172.20.22.202
172.20.0.0 172.20.22.96
```

Set ip route Command

Use the `set ip route` command to add IP addresses to the IP routing table.

The syntax for this command is:

```
set ip route <destination> <gateway>
```

<destination>	IP address of the network, or specific host to be added
<gateway>	IP address of the router.

Example:

This example shows how to add a default route to the IP routing table:

```
P130-1# set ip route 149.49.48.0 192.122.173.42
Route added.
```

Clear ip route Command

Use the `clear ip route` command to delete IP routing table entries.

The syntax for this command is:

```
clear ip route <destination> <gateway>
```

<destination>	IP address of the network, or specific host to be added
<gateway>	IP address of the router.

Example:

To delete the route table entries using the clear ip route command:

```
P130# clear ip route 134.12.3.0 192.1.1.1
Route deleted.
```

PPP Commands

To see the status of the PPP Interface, use the Show interface Command on page 49.

Show ppp session command

Use the show ppp session command to display PPP parameters and statistics of the current active PPP session.

The syntax for this command is:

```
show ppp session
```

Example:

```
P130-N> show ppp session
ppp0
        LCP Stats
                LCP phase                       ESTABLISH
                LCP state                       STOPPED
                passive                         ON
                silent                          ON
                restart                         OFF
                lcp echo timer                  OFF
        IPCP Stats
                IPCP state                      INITIAL
        PAP Stats
                client PAP state                INITIAL
                server PAP state                INITIAL
        CHAP Stats
                client CHAP state               INITIAL
                server CHAP state               INITIAL
```

Set interface ppp command

Use the `set interface ppp` command to configure the IP parameters of the device's PPP interface. No PPP connection can be established with the device until it is configured with a non-null IP address and net-mask. This IP address is a dummy address shared only between the two peers. It must be taken from an IP sub-net different than the IP sub-net of the agent.

The syntax for this command is:

```
set interface ppp <ip-address> <net-mask>
```

Example:

```
P130-1# set interface ppp 149.49.34.125 255.255.255.0
Interface PPP has its IP address set.
```

Set interface ppp enable | enable-always | disable | off | reset Command

Use the `set interface ppp` command to disconnect the PPP session, or to reset the connected modem. Use the provided on demand DB-25 to RJ45 connector for plugging-in the RJ-45 to RJ-45 delivered cable into the modem's DB-25 connector from one side, while the other cable's side RJ-45 connector should be plugged into the device's Console RJ-45 port of any box..

The syntax for this command is:&_

```
set interface ppp {enable | enable-always | disable | off |
reset}
```

enable	Enable the use of PPP, and thus to enter the modem mode.
enable-always	Entering the Modem mode every time that the proprietary modem cable is plugged into the console port.
disable	Disable the use of PPP, and thus to enter the terminal mode.
off	Keyword to disconnect the active PPP session.
reset	Keyword to reset the connected modem.

Example:

```
P130-1# set interface ppp off
PPP session disconnected.

P130-1# set interface ppp reset
PPP has reset the connected modem.
```

Show ppp authentication Command

Use the `show ppp authentication` command to display the authentication method used for PPP sessions. The shared chap-secret will be displayed only when accessed from the Technician level.

The syntax for this command is:

```
show ppp authentication
```

Example:

```
P130-N> show ppp authentication

PPP Authentication Parameters:
-----------------------------------------
Incoming: CHAP

P130-N> show ppp authentication

PPP Authentication Parameters:
-----------------------------------------
Incoming: CHAP
CHAP secret:    sodot
```

Set ppp authentication incoming Command

Use the `set ppp authentication incoming` command to define which authentication method will be used separately when doing a PPP server or client session.

The syntax for this command is:

```
set ppp authentication incoming {pap | chap | none}
```

incoming	Keyword for setting the authentication method used in PPP dial-in sessions.
pap	Keyword to use the PAP authentication method.
chap	Keyword to use the CHAP authentication method.
none	Keyword for performing no authentication.

Example:

```
P130-1# set ppp authentication incoming chap
PPP requires CHAP authentication for incoming sessions.
```

Set ppp chap-secret Command

Use the `set ppp chap-secret` command to configure the 'shared secret' used when CHAP authentication is used for PPP sessions. The chap-secret will not be transferable via the configuration upload/download mechanism.

The syntax for this command is:

```
set ppp chap-secret <chap-secret>
```

<chap-secret>	The shared secret used for CHAP authentication. It must be 4 to 8 characters long. CHAP authentication will not be used until a valid shared secret is entered.

Example:

```
P130-1# set ppp chap-secret sodot
PPP shared secret for CHAP authentication is set.
```

Show ppp incoming timeout Command

Use the `show ppp incoming timeout` command to display the amount of minutes a PPP dial-in session can remain idle before being automatically disconnected.

The syntax for this command is:

```
show ppp incoming timeout
```

Example:

```
P130-N> show ppp incoming timeout
PPP incoming timeout is 20 minutes.
```

Set ppp incoming timeout Command

Use the `set ppp incoming timeout` command to configure the number of minutes until the system automatically disconnects an idle PPP incoming session.

The syntax for this command is:

```
set ppp incoming timeout <timeout-in-minutes>
```

<timeout-in-minutes>	Number of minutes between 0 to 999 until the system automatically disconnects an idle PPP session. Setting the value to 0 disables the automatic disconnection of idle sessions. The default is no timeout.

Example:

```
P130-1# set ppp incoming timeout 20
PPP incoming sessions will automatically disconnect after 20
minutes of idle time.
```

Show ppp configuration Command

Use the `show ppp configuration` command to view the ppp configuration.

The syntax for this command is:

```
show ppp configuration
```

Example:

```
P130-N> show ppp configuration
PPP baud rate is 38400
PPP incoming timeout is 0 minutes
PPP Authentication Parameters:
------------------------------
Incoming:       PAP
```

Show ppp baud-rate Command

Use the `show ppp baud-rate` command to view the baud rate.

The syntax for this command is:

```
show ppp baud-rate
```

Example:

```
P130-N> show ppp baud-rate
PPP baud rate is 38400
```

Set ppp baud-rate Command

Use the `set ppp baud-rate` command to define the PPP baud rate to use. The peer baud-rate must be set to the same value.

The syntax for this command is:

```
set ppp baud-rate <9600 | 19200 | 38400>
```

Example:

```
P130-1# set ppp baud-rate 19200
```

Radius Commands

Show radius authentication Command

Use the `show radius authentication` command to display all RADIUS authentication configurations. The shared secrets will not be displayed.

The syntax for this command is:

```
show radius authentication
```

Example:

```
P130-N(super)# show radius authentication

RADIUS Authentication Parameters:
-------------------------------------------------
Mode:                                  Enabled
Primary-server:                  149.49.42.252
Secondary-server:                149.49.48.134
Retry-number:                                4
Retry-time:                                  5
UDP-port:                                 1645
shared-secret:                           sodot
```

Set radius authentication Command

Use the `set radius authentication` command to enable or disable authentication for the P130 unit. RADIUS authentication is disabled by default.

The syntax for this command is:

```
set radius authentication {enable | disable}
```

Set radius authentication secret Command

Use the `set radius authentication` command to enable secret authentication for the P130 unit.

The syntax for this command is:

```
set radius authentication secret <string>
```

<string>	Text password

Example:

```
P130-N(super)# set radius authentication secret sodot
```

Set radius authentication server Command

Use the `set radius authentication server` command to set a primary or secondary RADIUS server IP address.

The syntax for this command is:

```
set radius authentication server <ip-addr><primary|secondary>
```

<ip-addr>	IP address of the RADIUS authentication server
<primary>	Default - Primary authentication server
<secondary>	Secondary authentication server

Example:

```
P130-N(super)# set radius authentication server 149.49.38.12
primary
```

Clear radius authentication server Command

Use the `clear radius authentication server` command to remove a primary or secondary RADIUS authentication server.

The syntax for this command is:

```
clear radius authentication server[{primary|secondary}]]
```

primary	Primary authentication server
secondary	Secondary authentication server

Example:

```
P130-N(super)# clear radius authentication server primary
```

Set radius authentication retry-time Command

Use the `set radius authentication retry-time` command to set the time to wait before re-sending an access request.

The syntax for this command is:

```
set radius authentication retry time <time>
```

<time>	Retry time in seconds

Set radius authentication retry-number Command

Use the `set radius authentication retry-number` command to set the number of times an access request is sent when there is no response.

The syntax for this command is:

```
set radius authentication retry number <number>
```

<number>	Retry number

Set radius authentication udp-port Command

Use the `set radius authentication udp-port` command to set the RFC 2138 approved UDP port number. Normally, the UDP port number should be set to its default value of 1812. Some early implementations of the RADIUS server used port number 1645.

The syntax for this command is:

```
set radius authentication server udp-port <1812|1645>
```

RMON Commands

No rmon history Command

Use the `no rmon history` command to delete an existing RMON history entry.

The syntax for this command is:

```
no rmon history <History Index>
```

No rmon alarm Command

Use the `no rmon alarm` command to delete an existing RMON alarm entry.

The syntax for this command is:

```
no rmon alarm <Alarm Index>
```

No rmon event Command

Use the `no rmon event` command to delete an existing RMON event entry.

The syntax for this command is:

```
no rmon event <Event Index>
```

Rmon alarm Command

Use the `rmon alarm` command to create a new RMON alarm entry.

The syntax for this command is:

```
rmon alarm <Alarm Number> <variable> <interval> <sampletype>
rising-threshold <rising threshold> <rising event> falling-
threshold <falling threshold> <falling event> <startup alarm>
<owner>
```

<Alarm number>	The alarm index number of this entry (it is advisable to use the same interface number as your alarm index number.)
<variable>	The MIB variable which will be sampled by the alarm entry.
<interval>	The interval between 2 samples
<sample type>	Can be set to either **delta** (the difference between 2 samples) or an **absolute** value.

<rising threshold>	Sets the upper threshold for the alarm entry.
<rising event>	The RMON event entry that will be notified if the upper threshold is passed.
<falling threshold>	Sets the lower threshold for the alarm entry.
<falling event>	The RMON event entry that will be notified if the lower threshold is passed.
<startup alarm>	The instances in which the alarm will be activated. The possible parameters are: **Rising, Falling, risingOrfalling.**
<owner>	Owner name string

Example:

```
P130-1# rmon alarm 1026 1.3.6.1.2.1.16.1.1.1.5.1026 60 delta
rising-threshold 10000 1054 falling-threshold 10 1054
risingOrFalling amir
alarm 1026 was created successfully
```

Rmon event Command

Use the `rmon event` command to create an RMON event entry.

The syntax for this command is:

```
rmon event <Event Number> <type> description <description>
owner <owner>
```

<Event number>	The event index number of this entry.
<type>	The type of the event. The possible parameters are: **trap, log, logAndTrap, none.**
<description>	A user description of this event
<owner>	Owner name string

Example:

```
P130-1#  rmon event 1054 logAndTrap description "event for
monitoring amir's computer" owner amir
event 1054 was created successfully
```

Rmon history Command

Use the `rmon history` command to create an RMON history entry.

The syntax for this command is:

```
rmon history <history index> <interface> interval <interval>
buckets <number of buckets> owner <owner name>
```

<history_index>	The history index number of this entry (it is advisable to use the same interface number as your history index number.)
<interface>	The interface number is a unique number for each port which can be calculated as follows: 1024 x Module Number + Port Number For example: Port 3 in Module 1 has an Inter Number of 1027.
<interval>	The interval between 2 samples
<number of buckets>	The number of buckets defined
<owner name>	Owner name string

Example:

```
P130-1# rmon history 1026 1026 interval 30 buckets 20 owner
amir
history 1026 was created successfully
```

Show rmon history Command

Use the `show rmon history` command to show the most recent RMON history log for a given History Index. The history index is defined using the `rmon history` command (see Rmon history Command) or using an RMON management tool.

The syntax for this command is:

```
show rmon history [<History Index>]
```

Example:

```
P130-N> show rmon history 1026
history

Entry 1026 is active, owned by amir
Monitors ifEntry.1.1026 every 30 seconds
```

```
Requested # of time intervals, ie buckets, is 20
Granted # of time intervals, ie buckets, is 20
Sample # 1 began measuring at 2:53:9
Received 62545 octets, 642 packets,
391 broadcast and 145 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

Show rmon alarm Command

Use the `show rmon alarm` command to show the parameters set for a specific alarm entry that was set using the `rmon alarm` command or using the P130 Device Manager.

The syntax for this command is:

```
show rmon alarm [<Alarm Index>]
```

Example:

```
P130-N> show rmon alarm 1026
alarm

alarm 1026 is active, owned by amir
Monitors ifEntry.1.1026 every 60 seconds
Taking delta samples, last value was 1712
Rising threshold is 10000, assigned to event # 1054
Falling threshold is 10, assigned to event # 1054
On startup enable rising or_falling alarms
```

Show rmon event Command

Use the `show rmon event` command to show the parameters of an Event entry defined by the `rmon event` command or using the P130 Device Manager.

The syntax for this command is:

```
show rmon event [<Event Index>]
```

Example:

```
P130-N> show rmon event 1054
event
```

```
Event 1054 is active, owned by amir
Description is event for monitoring amir's co
Event firing causes log and trap to community public, last
fired 0:0:0
```

Show rmon statistics Command

Use the show rmon statistics command to show the RMON statistics counters for a certain interface number according to the MIB-2 interface table numbering scheme.

The syntax for this command is:

```
show rmon statistics <Interface Number>
```

Example:

```
P130-N> show rmon statistics 1026

statistics

Interface 1026 is active, owned by Monitor
Monitors ifEntry.1.1026 which has
Received 26375085 octets, 222536 packets,
154821 broadcast and 53909 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
1 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
# of packets received of length (in octets):
64:94530, 65-127:85124, 128-255:25896,
256-511:10440, 512-1023:6057, 1024-1518:489,
```

SNMP Commands

Show snmp Command

Use the `show snmp` command to display SNMP information.

The syntax for this command is:

```
show snmp
```

Example:

```
P130-N> show snmp
Authentication trap disabled

Community-Access     Community-String
----------------     ----------------
read-only            public
read-write           public
trap                 public

Trap-Rec-Address     Traps Enabled
----------------     ----------------
1.1.1.1              config
                     fault
etc...
```

Show snmp retries Command

Use the `show snmp retries` command to display the number of retries initiated by the Device Manager application when it tries to send SNMP messages to the device.

The syntax for this command is:

```
show snmp retries
```

Example:

```
P130-N> show snmp retries
the SNMP Retries Number is 3
```

Show snmp timeout Command

Use the `show snmp timeout` command to display the default SNMP timeout in seconds. This command is useful for access using the Device Manager.

The syntax for this command is:

```
show snmp timeout
```

Example:

```
P130-N> show snmp timeout
the SNMP Timeout is 2000
```

Set snmp community Command

Use the `set snmp community` command to set SNMP communities and associated access types.

There are three configurable SNMP communities, one for each access type. If you do not specify the community string, the string configured for that access type is cleared. One community string different from the default ("public") should be configured for *each* access type in order for secure SNMP access.

The syntax for this command is:

```
set snmp community {read-only|read-write|trap} [community_string]
```

read-only	Assign read-only access to the specified SNMP community.
read-write	Assign read-write access to the specified SNMP community.
trap	Assign SNMP community to trap.
community_string	(Optional) Name of the SNMP community. If no name is specified this command will clear any community for this access type.

The default configuration has the following communities and access types defined:

read-only – public

read-write – public

public-trap – public

Example:

To set read-write access to the SNMP community called snow:

```
P130-1# set snmp community read-write snow
SNMP read-write community string set.
```

To clear the community string defined for read-only access:

```
P130-1# set snmp community read-only
SNMP read-only community string cleared.
```

Set snmp retries Command

Use the `set snmp retries` command to set the number of retries initiated by the Device Manager application when it tries to send SNMP messages to the device.

The syntax for this command is:

set snmp retries <number>

<number>	Number of retries

Example:

```
P130-1# set snmp retries
```

Set snmp timeout Command

Use the `set snmp timeout` command to set the SNMP timeout in seconds. This command is useful for access using the Device Manager.

The syntax for this command is:

set snmp timeout <number>

<number>	Time in seconds

Example:

```
P130-1# set snmp timeout 2000
```

Set snmp trap auth Command

Use the `set snmp trap auth` commands to enable/disable the sending of SNMP traps upon SNMP authentication failure.

The syntax for this command is:

set snmp trap {enable|disable} **auth**

Example:

```
P130-1# set snmp trap enable auth
Authentication trap enabled
```

Set snmp trap Commands

Use the `set snmp trap` commands to add an entry into the SNMP trap receiver table and to enable or disable the different SNMP traps for a specific receiver. First add the `rcvr_addr` and then enable/disable the different traps for it.

The syntax for this command is:

```
set snmp trap <rcvr_addr>
set snmp trap <rcvr_addr> {enable|disable} {all|config|fault|...}
```

enable	Activate SNMP traps
disable	Deactivate SNMP traps
all	(Optional) Specify all trap types
config	(Optional) Specify the ConfigChange trap from the TRAP-MIB.
fault	(Optional) Specify the Fault trap from the TRAP-MIB.
rcvr_addr	IP address or IP alias of the system to receive SNMP traps

Example:

To enable SNMP ConfigChange traps to a specific manager:

```
P130-1# set snmp trap 192.122.173.42 enable config
SNMP config change traps enabled.
```

To enable all traps to a specific manager:

```
P130-1# set snmp trap 192.122.173.42 enable all
All SNMP traps enabled.
```

To disable SNMP config traps to a specific manager:

```
P130-1# set snmp trap 192.122.173.42 disable config
SNMP config traps disabled.
```

To add an entry in the SNMP trap receiver table with default:

```
P130-1# set snmp trap 192.122.173.42
SNMP trap receiver added.
```

Clear snmp trap Command

Use the `clear snmp trap` command to clear an entry from the SNMP trap receiver table.

The syntax for this command is:

```
clear snmp trap {<rcvr_addr>|all}
```

<rcvr_addr>	IP address or IP alias of the trap receiver (the SNMP management station) to clear.
all	Keyword that specifies every entry in the SNMP trap receiver table

Example:

```
P130-1# clear snmp trap 192.122.173.82
SNMP trap receiver deleted.
P130-1#
```

Policy Networking

The P130 is a policy workgroup switch which provides advanced policy-based networking at the edge of your network. The P130 implements Policy rules based on Layer 3 and Layer 4 header information. The policies are used to modify the Class of Service (CoS) of IP packets, which are sent by locally attached stations.

Policy Rules and Filters

Policy rules allow the user to define filtering rules which modify packet priority. Each packet is evaluated against a set of rules. The following criteria are used to develop rules:

- Source IP address
- Source IP address host mask
- Destination IP address
- Destination IP address host mask
- Protocol type
- Layer 4 source port range
- Layer 4 destination port range
- DSCP word
- TCP Ack Bit

There are 3 ways to define Policy rules:

- Locally using CLI commands
- Via the MultiService Network Manager EZ2Rule Policy Manager
- Via the Avaya policy application.

Using Policy Lists

- The P130 supports up to 128 policy rules from up to 8 policy rule types (i.e. Filters).
- You can configure up to 2 Policy Lists in a P130 module. Only one of them can be used as the Active List, while the other one is dormant.
- You can edit only the dormant rules list.

Note: Multilayer Policy support, beyond the basic P130 Layer 2 switch features requires a license key for activation. If no Multilayer Policy License Key was entered to the P130 switch, the Policy commands will not be activated.

Policy-based Networking Commands

Show access-group Command

Use the show `access-group` command to see information about the configured active access list.

The syntax for this command is:

`show access-group`

```
Example:
P130-N>  show access-group
access-group 100
```

Show ip access-lists Command

Use the `show ip access-lists` command to see all the current policy lists.

The syntax for this command is:

`show [ip] access-lists`

Example:

```
P130-N>  show ip access-lists
The current policy source is local

List 100 status is unkown(0)
ip access-list 100 1 fwd5 tcp
  any
  any range   500   503

ip access-list 100 2 fwd5 tcp
  host 149.49.0.0
  host 157.48.0.0      range  2000  2007

ip access-list 100 3 fwd7 udp
  any
  any eq       25

default action for list 100 is permit
```

Show dscp Command

Use the `show dscp` command to see the DSCP table.

The syntax for this command is:

`show dscp`

Example:

```
P130-1# show dscp
set qos trust trust-cos
DSCP table validity status: Valid
DSCP Action Precedence ApplicStatus   ApplicType     Name
---- ------ ---------- ------------- ------------- ----------
   5  fwd3  mandatory  applicable       quasi-static  DSCP #5
  21  fwd6  mandatory  applicable       quasi-static DSCP #21
  45  fwd7  mandatory  applicable       quasi-static DSCP #45
  60  fwd1  mandatory  applicable       quasi-static DSCP #60
```

ip access-group Command

Use the `ip access-group` command to activate a specific policy list. To deactivate the policy list, use the no version of this command.

The syntax for this command is:

`[no] [ip] access-group` `<policy-list-number>[<default-action>]`

<priority-list-number>	Integer (100..199)
<default-action>	default-action-deny | default-action-permit

```
P130-1# ip access-group 101
Policy list 101 was activated successfully
```

ip access-list Command

Use the `ip access-list` command to create a specific policy rule. This command defines a policy rule. The access list contains several of these rules. Each rule pertains to the source IP address, the destination IP address, the protocol, the protocol ports (if relevant), and to the ACK bit (if relevant). To delete a specific rule, use the `no` form of this command.

The syntax for this command is:

```
[no] [ip] access-list <access-list-number> <access-list-index>
         <command> <protocol> {<source-ip>
                    <source-wildcard> | any |host
                    <source-ip>}[<operator> <port> [<port]]
                    {<destination-ip> <destination-
                      wildcard>|any |host
                    <destination-ip>}[<operator> <port>
                   [<port>]][established] [precedence]
```

<access-list-number>	Integer (100..199)
<access-list-index>	Integer (1...9999)
<command>	permit | deny | deny-and-notify | fwd0-7
<protocol>	ip | tcp | udp | integer (1..255)
<source-ip>	IP network
<source-wildcard>	IP network wildcard
<operator>	eq | lt | gt | range
<port>	Integer (1..65535)
<destination-ip>	IP network
<destination-wildcard>	IP network wildcard
<precedence>	mandatory | optional]

Example:

```
P130-1# ip access-list 100 2 fwd5 tcp  host 149.49.0.0 host
157.48.0.0
```

Example:

```
P130-1# ip access-list 100 3 fwd7 udp any any eq 25
```

ip access-list-copy Command

Use the `ip access-list-copy` command to copy a policy rules list.

The syntax for this command is:

```
ip access-list-copy <source-list> <destination-list>
```

<source-list>	Integer (100..199)
<destination-list>	Integer (100..199)

Example:

```
P130-1# ip access-list-copy 100 101
Done!
P130-1#
```

ip access-default-action Command

Use the `ip-access-default action` command to set the default action for a specific policy list.

The syntax for this command is:

```
ip access-default-action <policy-list-number> <default-
action>
```

<policy-list-number>	Integer (100..199)
<default-action>	default-action-deny | default-action-permit

Example:

```
P130-1# ip access-default-action 101 default-action-deny
```

ip access-list-name Command

Use the `ip access-list-name` command to set a name for a policy list.

The syntax for this command is:

```
ip access-list-name <policy-list-number> <name>
```

<policy-list-number>	Integer (100..199)
<name>	List name

Example:

```
P130-1# ip access-list-name 101 morning
```

ip access-list-owner Command

Use the `ip access-list-owner` command to set the owner for a specific policy list.

The syntax for this command is:

```
ip access-list-owner <policy-list-number> <owner>
```

<policy-list-number>	Integer (100..199)
<owner>	List owner

```
P130-1# ip access-list-owner 101 admin
```

ip access-list-cookie Command

Use the `ip access-list-cookie` command to set the list cookie for a specific policy list.

The syntax for this command is:

```
ip access-list-cookie <policy-list-number> <cookie>
```

<policy-list-number>	Integer (100..199)
<cookie>	Integer

Example:

```
ip access-list-owner 101 12345
```

Validate-group Command

Use the `validate-group` command to verify that all the rules in a priority list are valid.

If there is a configuration problem with a specific rule, or with a number of rules, detailed error messages will be given.

The syntax for this command is:

```
validate-group <policy-list-number>[quiet]
```

quiet	Does not display error messages

```
Example:
P130-N(super)# validate-group 101
```

Set qos policy-source Command

Use the `set qos policy-source` command to set the policy source. The default policy source is policy-server.

Note: Before configuring the IP access list, you must change the policy source mode to local.

The syntax for this command is:

```
set qos policy-source <source>
```

<source>	local | policy-server

Example:

```
P130-N(super)# set qos policy-source local
```

Set qos dscp-cos-map Command

Use the `set qos dscp-cos-map` command to configure the DSCP table.

The syntax for this command is:

```
set qos dscp-cos-map <dscp1>[-<dscp2>] <operation>
```

<dscp1>	DSCP range min (0-63)
<dscp2>	DSCP range max (0-63)
<operation>	fwd0-7|no-change where fwd0-7 - forward this packet with priority level from 0 to 7, and no-change - do not change the priority level

Example:

```
P130-N(super)# set qos dscp-cos-map 9-11 fwd3
```

Example:

```
P130-N(super)# set qos dscp-cos-map  8 fwd7
```

Set qos dscp-name Command

Use the `set qos dscp-name` command to configure the DSCP entry name.

The syntax for this command is:

```
set qos dscp-name <dscp> <name>
```

<dscp>	DSCP entry (0-63)
<name>	Entry name

Example:

```
P130-N(super)# set qos dscp-name 10 "special"
```

Set qos trust Command

Use the `set qos trust` command to configure which of the incoming packet's priority parameters should be considered when determining the new assigned priority. You can configure the P130 to trust either the cos (the 802.1p priority), or the dscp (the DSCP value). The default value is trust-cos.

The syntax for this command is:

```
set qos trust {untrusted  | trust-cos | trust-dscp | trust-cos-dscp}
```

Note: The untrusted and trust-cos-dscp options are not operational on the P130.

Example:

```
P130-N(super)#  set qos trust dscp
```

IP port range upper limit for Command

Use the `ip port range upper limit for` command to determine the valid port range in a list.

The syntax for this command is:

```
ip port range upper limit for <lower_limit>
```

Example:

```
P130-N(super)# ip port range upper limit for 2048
Upper limit options:
2048,2049,2051,2055,2063,2079,2111,2175,2303,2559,3071,4095
```

Avaya P130 Embedded Web Manager

The Avaya P130 Embedded Web Manager provides the following:

- Device Configuration - Viewing and modifying the different device configurations.
- Virtual LANs - Viewing and editing Virtual LAN information.
- Link Aggregation Groups (LAGs) - Viewing and editing LAG information.
- Software Redundancy - Setting software redundancy for ports in a P130 Switch.
- Port Mirroring - Setting up port mirroring for ports in a P130 Switch.
- Trap Managers Configuration - Viewing and modifying the Trap Managers Table.
- Switch Connected Addresses - View devices connected to selected ports.
- IP Multicast filtering with IGMP snooping.
- Redundancy between LAGs
  - Also operates as a result of a module fault, e.g., power failure.

System Requirements

Minimum hardware and Operating System requirements are:

- Windows® 2000 or NT® 4.0 or higher
- Pentium® 200-Mhz-based, computer with 64 Mb of RAM (Pentium-II recommended)
- Minimum screen resolution of 1024 x 768 pixels
- Microsoft® Internet Explorer 4 or higher **or** Netscape Navigator® 4.*x* or higher
- Sun Microsystems Java™ plug-in version 1.3.1 (supplied)

Note for users of Netscape Navigator: The Java plug-in requires certain services from **Windows 95** which are not present if **Internet Explorer** is not installed. In order to add these services to the operating system, please install Internet Explorer version 3 or higher. You can then use either browser to manage the switch.

Running the Embedded Manager

Note: You should assign an IP address to the switch before beginning this procedure.

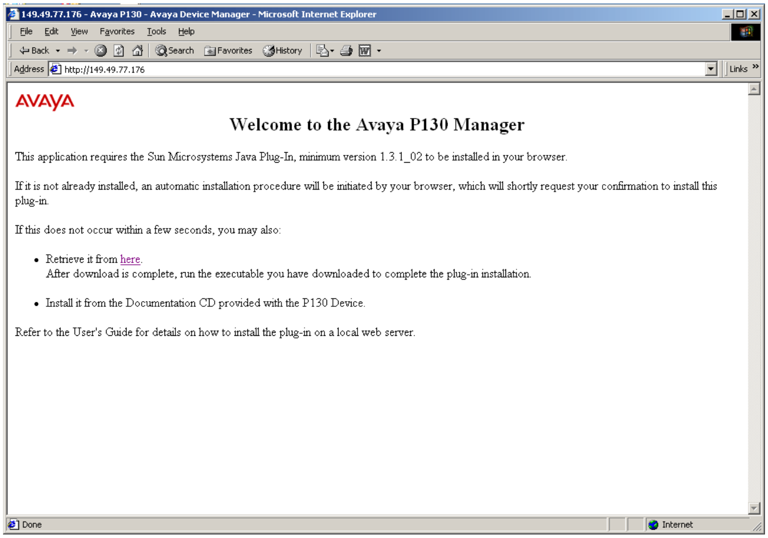
1 Open your browser.
2 Enter the url of the switch in the format **`http://`*`aaa.bbb.ccc.ddd`*** where ***`aaa.bbb.ccc.ddd`*** is the IP address of the switch.

Note: The user name is "root"
The default password for read-write access is "root".

Note: The Web management passwords are the same as those of the CLI. If you have created additional CLI user names or changed the default passwords then you can use those passwords for Web management as well.

The welcome page is displayed:

Figure A.1 The Welcome Page



http://149.49.77.176

Welcome to the Avaya P130 Manager

This application requires the Sun Microsystems Java Plug-In, minimum version 1.3.1_02 to be installed in your browser.

If it is not already installed, an automatic installation procedure will be initiated by your browser, which will shortly request your confirmation to install this plug-in.

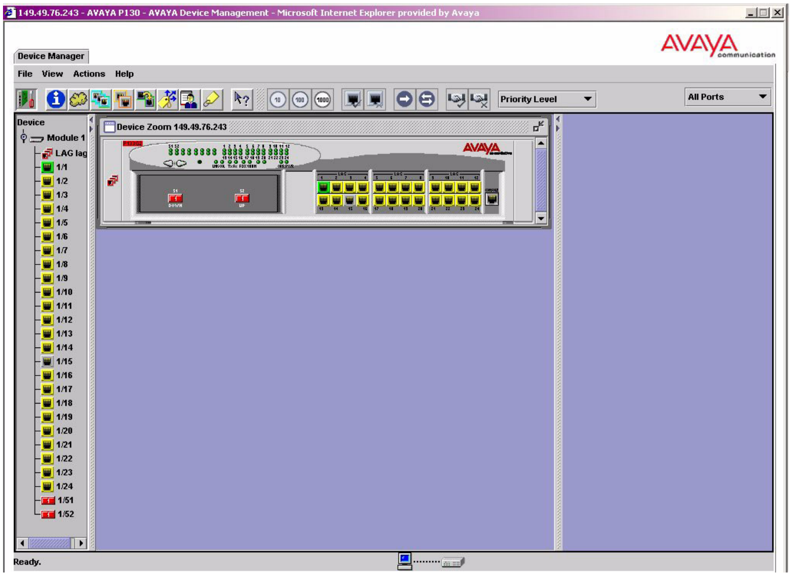
If this does not occur within a few seconds, you may also:

- Retrieve it from here.
  After download is complete, run the executable you have downloaded to complete the plug-in installation.
- Install it from the Documentation CD provided with the P130 Device.

Refer to the User's Guide for details on how to install the plug-in on a local web server.

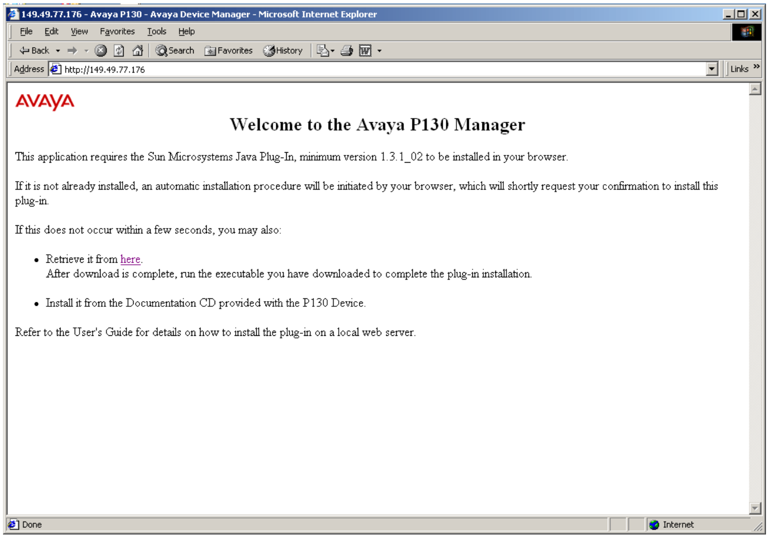
— If you have the Java plug-in installed, the Web-based manager should open in a new window (see Figure A.2).

Figure A.2 Web-based Manager



— If you do **not** have the Java plug-in installed, follow the instructions on the Welcome page that offers a variety of options to install the plug-in (see Figure A.3).

Figure A.3 Options for Installing the Java Plug-in



Welcome to the Avaya P130 Manager

This application requires the Sun Microsystems Java Plug-In, minimum version 1.3.1_02 to be installed in your browser.

If it is not already installed, an automatic installation procedure will be initiated by your browser, which will shortly request your confirmation to install this plug-in.

If this does not occur within a few seconds, you may also:

- Retrieve it from here.
  After download is complete, run the executable you have downloaded to complete the plug-in installation.
- Install it from the Documentation CD provided with the P130 Device.

Refer to the User's Guide for details on how to install the plug-in on a local web server.

Installing the Java Plug-in

If the network manager has configured the system, the plug-in should be installed automatically.

If the plug-in is not installed automatically, then you have three options for installing it manually:

Installing from the Avaya P130 Documentation and Utilities CD

1. Close all unnecessary applications on your PC.
2. Insert the “P130 Documentation and Utilities” CD into the CD drive.
3. Click **Start** on the task bar.
4. Select Run.
5. Type ***x:*\emweb-aux-files\plug-in_1_3_1.exe** where ***x:*** is the CD drive letter.
6. Follow the instructions on screen.

Install from the Avaya Site

Click on the link in the Welcome page.

Install from your Local Web Site

Click on the link in the Welcome page.

Note: This option is only available if the network manager has placed the files on the local Web server.

Installing the On-Line Help and Java Plug-In on your Web Site

Note: This procedure is optional.

Copying the help files and Java plug-in to a local Web server allows users to access the on-line help for the Embedded Manager and enables automatic installation of the Java plug-in the first time the users tries to manage the device.

1 Copy the `emweb-aux-files` directory from the “P130 Documentation and Utilities” CD to your local Web server. Following is a list of instructions for Windows NT. If your Web server is not an NT server please refer to your Web server documentation for full instructions.

   a Click **Start -> Programs -> Microsoft Peer Web Services (Common) -> Internet Services Manager.**

   b Double-click on the WWW service – this will open the WWW service properties.

   c Choose the Directories tab and click on Add.

   d In the Directory field enter the full Path to the `emweb-aux-files` you copied in step 1.

   e In the Alias field under the Virtual Directory option type: `emweb-aux-files` and click OK.

   f Close all open windows.

2 Define the URL in the P130 using the following CLI command:
`set web aux-files-url` ***`IP address/directory name`***
where ***`IP address/directory name`*** is the location of the directory from the previous step.

Documentation

The Device Manager comes with a detailed User’s Guide including a Glossary of Terms and an overview of Data Communications concepts.

Software Download

You can perform software download using the CLI or Avaya Update Manager (part of the MultiService Network Manager Suite).

Specifications

Avaya P130 Switches

Physical

Height	2U (88 mm, 3.5”)
Width	482.6 mm (19”)
Depth	350 mm(13.8”)
Weight	**P133T/G2/GT2/F2** - 5.2 kg (11.4 lb) **P134G2** - 6 kg (13.2 lb)

Power Requirements — AC

Input voltage	100 to 240 VAC, 50/60 Hz
Power consumption	**P133T/G2/GT2/F2 -** 50 W max **P134G2** - 66 W max
Input current	2 A@100 VAC 1 A@200 VAC
Inrush current	25 A@100 VAC (max.) 50 A@200VAC (max.)

Environmental

Operating Temp.	-5 to 50°C (23 to 122°F)
Rel. Humidity	5% to 95% non-condensing

Interfaces

- **P133T**
  - — 24 x 10/100BASE-TX RJ45 port connectors.
  - — RS-232 for terminal setup via RJ45 connector on front panel.
- **P133F2**
  - — 24 x 10/100BASE-TX RJ45 port connectors.
  - — Two 100FX connectors.
  - — RS-232 for terminal setup via RJ45 connector on front panel.
- **P133G2**
  - — 24 x 10/100BASE-TX RJ45 port connectors.
  - — Two SFP Gigabit transceiver housings for SFF/SFP mini GBIC.
  - — RS-232 for terminal setup via RJ45 connector on front panel.
- **P134G2**
  - — 48 x 10/100BASE-TX RJ45 port connectors.
  - — Two SFP Gigabit transceiver housings for SFF/SFP mini GBIC.
  - — RS-232 for terminal setup via RJ45 connector on front panel.
- **P133GT2**
  - — 24 x 10/100BASE-TX RJ45 port connectors.
  - — Two 100/1000BaseT RJ45 port connectors.
  - — RS-232 for terminal setup via RJ45 connector on front panel.

Basic MTBF

P133T	331,901 hrs minimum
P133F2	215,597 hrs minimum
P133G2	253,386 hrs minimum
P134G2	223,815 hrs minimum
P133GT2	278,316 hrs minimum

Safety

- UL for US approved according to UL195O Std.
- C-UL(UL for Canada) approved according to C22.2 No.950 Std.
- CE for Europe approved according to EN 60950 Std.
- Laser components are “Class 1 Laser Products”:
  - — EN-60825/IEC-825-1 for Europe
  - — FDA 21 CFR 1040.10 and 1040.11 for USA.
- Overcurrent Protection: A readily accessible listed safety-approved protective device with a 16A rating must be incorporated in series with building installation AC power wiring for the equipment under protection.

EMC Emissions

Emissions

Approved according to:

- US -FCC Part 15 sub part B, class A
- Europe - EN55022 class A & EN61000-3-2
- Japan - VCCI-A

Immunity

Approved according to:

- EN55024
- E 61000-3-3

Avaya Approved SFF/SFP GBIC Transceivers

This SFF/SFP GBIC (Gigabit Interface Converter) has been tested for use with Avaya's P133G2 Gbit/s Gigabit Ethernet ports.

Note: SFF/SFP GBIC transceivers are hot-swappable.

Safety Information

The SFF/SFP GBIC transceivers are Class 1 Laser products. They comply with EN 60825-1 and Food and Drug Administration (FDA) 21 CFR 1040.10 and 1040.11.

The SFF/SFP GBIC transceivers must be operated under recommended operating conditions.

Laser Classification

CLASS 1
LASER PRODUCT

Note: Class 1 lasers are inherently safe under reasonably foreseeable conditions of operation.

Caution: The use of optical instruments with this product will increase eye hazard.

Usage Restriction

When a SFF/SFP GBIC transceiver is inserted in the module but is not in use, the Tx and Rx ports should be protected with an optical connector or a dust plug.

Caution: Use only Avaya approved SFF/SFP GBIC transceivers. All approved SFF/ SFP GBIC transceivers:
1) Are 3.3V. Do **not** insert a 5V SFF/SFP GBIC.
2) Use Serial Identification. Do **not** use a GBIC that utilizes Parallel Identification.

Installation

Installing and Removing a SFF/SFP GBIC Transceiver

Caution: Use only 3.3V Avaya-authorized SFF/SFP GBIC transceivers.
Use only SFF/SFP GBIC transceivers that use Serial Identification.

The SFF/SFP GBIC transceiver is fastened using a snap-in clip.

To Install the SFF/SFP GBIC tranceiver:

- Insert the transceiver (take care to insert it the right way up) until it clicks in place.

To Remove the SFF/SFP GBIC tranceiver:

1 Press the clip on the bottom side of the transceiver.
2 Pull the transceiver out.

Specifications

LX Transceiver

A 9 µm or 10 µm single-mode fiber (SMF) cable may be connected to a 1000Base-LX SFF/SFP GBIC port. The maximum length is 10 km (32,808 ft).

A 50 µm or 62.5 µm multimode (MMF) fiber cable may be connected to a 1000Base-LX SFF/SFP GBIC port. The maximum length is 550 m (1,804 ft.) for 50 µm and 62.5 µm cable.

The LX transceiver has a Wavelength of 1300 nm, Transmission Rate of 1.25 Gbps, Input Power of 3.3V, and Maximum Output Wattage of -3 dBm.

SX Transceiver

A 50 µm or 62.5 µm multimode (MMF) fiber cable may be connected to a 1000Base-SX SFF/SFP GBIC port. The maximum length is 500 m (1,640 ft.) for 50 µm and 220 m (722 ft.) for 62.5 µm cable.

The SX transceiver has a Wavelength of 850 nm, Transmission Rate of 1.25 Gbps, Input Power of 3.3V, and Maximum Output Wattage of -4 dBm.

Agency Approval

The transceivers comply with:

- EMC Emission: US – FCC Part 15, Subpart B, Class A;
  Europe – EN55022 class A
- Immunity: EN50082-1

Safety: UL for US UL 1950 Std., C-UL (UL for Canada) C22.2 No.950 Std., Food and Drug Administration (FDA) 21 CFR 1040.10 and 1040.11, and CE for Europe EN60950 Std. Complies with EN 60825-1.

Connector Pin Assignments

Console Communications

For direct Console communications, connect the Avaya P130 to the Console Terminal using the supplied RJ-45 crossed cable and RJ-45 to DB-9 adapter.

For remote Console communications through a dial-up modem, connect the P130 to a modem using the supplied RJ-45 cross cable and RJ-45 to DB-25 adapter.

Table B.1 Pinout of the Required Connection for Console Communications

P130 RJ-45 Pin	Name	Terminal DB-9 Pins	Modem DB-25 Pin
1	For Future Use	NC	[1](see Footnote)
2	TXD (P130 input)	3	3
3	RXD (P130 output)	2	2
4	CD	4	8
5	GND	5	7
6	DTR	1	20
7	RTS	8	4
8	CTS	7	5

[1] Pin 1 of the Modem DB-25 connector is internally connected to Pin 7 GND

Appendix C

Index of all CLI Commands

CLI Command Set

The CLI commands are listed below in alphabetical order. Each of the commands listed here is linked to the command description in this manual.

How to Contact Us

To contact Avaya's technical support, please call:

In the United States

Dial 1-800-237-0016, press 0, then press 73300.

In the EMEA (Europe, Middle East and Africa) Region

Country	Local Dial-In Number
Albania	+31 70 414 8001
Austria	+43 1 36 0277 1000
Azerbaijan	+31 70 414 8047
Bahrain	+800 610
Belgium	+32 2 626 8420
Belorussia	+31 70 414 8047
Bosnia Herzegovina	+31 70 414 8042
Bulgaria	+31 70 414 8004
Croatia	+31 70 414 8039
Cyprus	+31 70 414 8005
Czech Rep.	+31 70 414 8006
Denmark	+45 8233 2807
Egypt	+31 70 414 8008
Estonia	+372 6604736
Finland	+358 981 710 081

Country	Local Dial-In Number
France	+33 1 4993 9009
Germany	+49 69 95307 680
Ghana	+31 70 414 8044
Gibraltar	+31 70 414 8013
Greece	+00800 3122 1288
Hungary	+06800 13839
Iceland	+0800 8125
Ireland	+353 160 58 479
Israel	+1 800 93 00 900
Italy	+39 02 7541 9636
Jordan	+31 70 414 8045
Kazakhstan	+31 70 414 8020
Kenya	+31 70 414 8049
Kuwait	+31 70 414 8052
Latvia	+371 721 4368

Country	Local Dial-In Number
Lebanon	+31 70 414 8053
Lithuania	+370 2 756 800
Luxemburg	+352 29 6969 5624
Macedonia	+31 70 414 8041
Malta	+31 70 414 8022
Mauritius	+31 70 414 8054
Morocco	+31 70 414 8055
Netherlands	+31 70 414 8023
Nigeria	+31 70 414 8056
Norway	+47 235 001 00
Oman	+31 70 414 8057
Pakistan	+31 70 414 8058
Poland	+0800 311 1273
Portugal	+351 21 318 0047
Qatar	+31 70 414 8059
Romania	+31 70 414 8027
Russia	+7 095 733 9055
Saudi Arabia	+31 70 414 8022

Country	Local Dial-In Number
Slovakia	+31 70 414 8066
Slovania	+31 70 414 8040
South Africa	+0800 995 059
Spain	+34 91 375 3023
Sweden	+46 851 992 080
Switzerland	+41 22 827 8741
Tanzania	+31 70 414 8060
Tunisia	+31 70 414 8069
Turkey	+800 4491 3919
UAE	+31 70 414 8036
Uganda	+31 70 414 8061
UK	+44 0207 5195000
Ukraine	+31 70 414 8035
Uzbekistan	+31 70 414 8046
Yemen	+31 70 414 8062
Yugoslavia	+31 70 414 8038
Zimbabwe	+31 70 414 8063

Email: csctechnical@avaya.com

In the AP (Asia Pacific) Region

Country	Local Dial-In Number
Australia	+1800 255 233
Hong Kong	+2506 5451
Indonesia	+800 1 255 227
Japan	+0 120 766 227
Korea	+0 80 766 2580

Country	Local Dial-In Number
Malaysia	+1800 880 227
New Zealand	+00 800 9828 9828
Philippines	+1800 1888 7798
Singapore	+1800 872 8717
Taiwan	+0 80 025 227

Email: sgcoe@avaya.com

In the CALA (Caribbean and Latin America) Region

Email: caladatasupp@avaya.com

Hot Line:+1 720 4449 998

Fax:+1 720 444 9103

For updated information, visit www.avayanetwork.com, and click “Global Support Organization (GSO)”.

All trademarks, registered trademarks, service names, product and/or brand names are the sole property of their respective owners.

Copyright © 2002 Avaya Inc. All rights reserved.